

Министерство образования и науки Российской Федерации
ФГБОУ ВО «Уральский государственный педагогический университет»
Институт математики, информатики и информационных технологий
Кафедра высшей математики

**Решеточная характеристика подалгебр, матричных алгебр,
рассматриваемых над конечным полем**

Выпускная квалификационная работа

Квалификационная работа
допущен к защите
Зав. кафедрой

Исполнитель:
Бурдыко Виталий Максимович,
обучающийся Б-42 группы

дата

подпись

подпись

Руководитель ОПОП:

Научный руководитель:
Коробков С.С.,
к.ф.-м.н., доцент

подпись

подпись

Екатеринбург 2017

Оглавление

Введение	3
ГЛАВА I. Теоретические основы	6
1. Основные алгебраические структуры	6
2. Алгебры над полем.....	15
3. Решетки	20
ГЛАВА II. Система компьютерной алгебры GAP	25
1. Общая характеристика	25
2. Язык программирования GAP	27
3. Команды для вычислений в GAP используемые в работе	28
4. Простейшие программы для вычислений в матричных алгебрах	29
ГЛАВА III. Решеточная характеристика четырехмерных подалгебр, алгебры $A=M(GF(2),3)$	34
1. Понятие типа решетки	34
2. Алгоритм построения диаграммы решетки подалгебр.....	48
3. Построение диаграмм	52
Библиографический список.....	58
Приложения	59

Введение

В выпускной квалификационной работе рассматривается алгебра $A = M_3(GF(2))$ квадратных матриц порядка 3 над полем из двух элементов. Основным объектом исследования является четырехмерные подалгебры алгебры A . Для каждого таких подалгебр изображаются диаграммы решеток их подалгебр.

Актуальность выбора темы: заключается в необходимости создания большой базы примеров конечномерных алгебр с различными алгебраическими свойствами и типами решеток подалгебр.

Целью исследования является разработка алгоритмов и программ для получения классификации четырехмерных подалгебр алгебры A по типам их решеток подалгебр.

Достижение основной цели осуществляется с помощью решения следующих задач: используя систему компьютерной алгебры **GAP**

1. найти все четырехмерные подалгебры в алгебре A ;
2. определить типы решеток найденных подалгебр;
3. классифицировать с точностью до изоморфизма алгебры, имеющие один тот же тип решетки подалгебр.

Работа состоит из введения, трех глав, списка литературы и приложений.

Первая глава носит теоретический характер. В ней приведены основные алгебраические структуры: группы, кольца, поля, алгебры над полем. Приводятся примеры алгебр, понятие подалгебры и признак подалгебры. Здесь же приведено определение решетки, указаны основные свойства решеток.

Так как все вычисления проводятся в системе компьютерной алгебры **GAP**, во второй главе приводится общая характеристика этой системы и основные ее команды. Представлены простейшие программы для вычислений в матричных алгебрах.

Третья глава содержит практическую часть. В ней представлены четырехмерные подалгебры алгебры $M_3(GF(2))$, приводится их полная классификация. Находятся решетки подалгебр и их типы. Основные результаты, полученные в работе, приведены в таблице № 1.

Таблица №1

Тип подалгебры	Порождающие элементы	Определяющие соотношения	Количество подалгебр	Тип решетки подалгебр																									
1	e_1, e_2, r_1, r_2	<table border="1"> <tr><td>·</td><td>e_1</td><td>e_2</td><td>r_1</td><td>r_2</td></tr> <tr><td>e_1</td><td>e_1</td><td>0</td><td>r_1</td><td>r_2</td></tr> <tr><td>e_2</td><td>0</td><td>e_2</td><td>0</td><td>0</td></tr> <tr><td>r_1</td><td>r_1</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>r_2</td><td>0</td><td>r_2</td><td>0</td><td>0</td></tr> </table>	·	e_1	e_2	r_1	r_2	e_1	e_1	0	r_1	r_2	e_2	0	e_2	0	0	r_1	r_1	0	0	0	r_2	0	r_2	0	0	42	(1,8,12,6,1)
·	e_1	e_2	r_1	r_2																									
e_1	e_1	0	r_1	r_2																									
e_2	0	e_2	0	0																									
r_1	r_1	0	0	0																									
r_2	0	r_2	0	0																									
2	e_1, e_2, r_1, r_2	<table border="1"> <tr><td>·</td><td>e_1</td><td>e_2</td><td>r_1</td><td>r_2</td></tr> <tr><td>e_1</td><td>e_1</td><td>0</td><td>r_1</td><td>0</td></tr> <tr><td>e_2</td><td>0</td><td>e_2</td><td>0</td><td>r_2</td></tr> <tr><td>r_1</td><td>r_1</td><td>r_2</td><td>0</td><td>0</td></tr> <tr><td>r_2</td><td>0</td><td>0</td><td>0</td><td>0</td></tr> </table>	·	e_1	e_2	r_1	r_2	e_1	e_1	0	r_1	0	e_2	0	e_2	0	r_2	r_1	r_1	r_2	0	0	r_2	0	0	0	0	42	(1,8,12,6,1)
·	e_1	e_2	r_1	r_2																									
e_1	e_1	0	r_1	0																									
e_2	0	e_2	0	r_2																									
r_1	r_1	r_2	0	0																									
r_2	0	0	0	0																									
3	e_1, e_2, r_1, r_2	<table border="1"> <tr><td>·</td><td>e_1</td><td>e_2</td><td>r_1</td><td>r_2</td></tr> <tr><td>e_1</td><td>e_1</td><td>0</td><td>r_1</td><td>0</td></tr> <tr><td>e_2</td><td>0</td><td>e_2</td><td>0</td><td>r_2</td></tr> <tr><td>r_1</td><td>0</td><td>r_1</td><td>0</td><td>e_1</td></tr> <tr><td>r_2</td><td>r_2</td><td>0</td><td>e_2</td><td>0</td></tr> </table>	·	e_1	e_2	r_1	r_2	e_1	e_1	0	r_1	0	e_2	0	e_2	0	r_2	r_1	0	r_1	0	e_1	r_2	r_2	0	e_2	0	28	(1,10,13,3,1)
·	e_1	e_2	r_1	r_2																									
e_1	e_1	0	r_1	0																									
e_2	0	e_2	0	r_2																									
r_1	0	r_1	0	e_1																									
r_2	r_2	0	e_2	0																									
4	e_1, e_2, r_1, r_2	<table border="1"> <tr><td>·</td><td>e_1</td><td>e_2</td><td>r_1</td><td>r_2</td></tr> <tr><td>e_1</td><td>e_1</td><td>0</td><td>r_1</td><td>r_2</td></tr> <tr><td>e_2</td><td>0</td><td>e_2</td><td>0</td><td>0</td></tr> <tr><td>r_1</td><td>0</td><td>r_1</td><td>0</td><td>e_1</td></tr> <tr><td>r_2</td><td>0</td><td>0</td><td>e_2</td><td>0</td></tr> </table>	·	e_1	e_2	r_1	r_2	e_1	e_1	0	r_1	r_2	e_2	0	e_2	0	0	r_1	0	r_1	0	e_1	r_2	0	0	e_2	0	42	(1,11,17,7,1)
·	e_1	e_2	r_1	r_2																									
e_1	e_1	0	r_1	r_2																									
e_2	0	e_2	0	0																									
r_1	0	r_1	0	e_1																									
r_2	0	0	e_2	0																									

5	e_1, e_2, r_1, r_2	<table> <tr><td>\cdot</td><td>e_1</td><td>e_2</td><td>r_1</td><td>r_2</td></tr> <tr><td>e_1</td><td>e_1</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>e_2</td><td>0</td><td>e_2</td><td>r_1</td><td>0</td></tr> <tr><td>r_1</td><td>r_1</td><td>r_2</td><td>0</td><td>e_1</td></tr> <tr><td>r_2</td><td>0</td><td>0</td><td>e_2</td><td>0</td></tr> </table>	\cdot	e_1	e_2	r_1	r_2	e_1	e_1	0	0	0	e_2	0	e_2	r_1	0	r_1	r_1	r_2	0	e_1	r_2	0	0	e_2	0	42	(1,11,17,7,1)
\cdot	e_1	e_2	r_1	r_2																									
e_1	e_1	0	0	0																									
e_2	0	e_2	r_1	0																									
r_1	r_1	r_2	0	e_1																									
r_2	0	0	e_2	0																									
6	e_1, e_2, r_1, r_2	<table> <tr><td>\cdot</td><td>e_1</td><td>e_2</td><td>r_1</td><td>r_2</td></tr> <tr><td>e_1</td><td>e_1</td><td>0</td><td>0</td><td>r_2</td></tr> <tr><td>e_2</td><td>0</td><td>e_2</td><td>r_1</td><td>0</td></tr> <tr><td>r_1</td><td>0</td><td>0</td><td>0</td><td>e_1</td></tr> <tr><td>r_2</td><td>0</td><td>0</td><td>e_2</td><td>0</td></tr> </table>	\cdot	e_1	e_2	r_1	r_2	e_1	e_1	0	0	r_2	e_2	0	e_2	r_1	0	r_1	0	0	0	e_1	r_2	0	0	e_2	0	21	(1,11,17,7,1)
\cdot	e_1	e_2	r_1	r_2																									
e_1	e_1	0	0	r_2																									
e_2	0	e_2	r_1	0																									
r_1	0	0	0	e_1																									
r_2	0	0	e_2	0																									
7	e_1, e_2, r_1, r_2	<table> <tr><td>\cdot</td><td>e_1</td><td>e_2</td><td>r_1</td><td>r_2</td></tr> <tr><td>e_1</td><td>e_1</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>e_2</td><td>0</td><td>e_2</td><td>0</td><td>0</td></tr> <tr><td>r_1</td><td>0</td><td>r_1</td><td>0</td><td>e_1</td></tr> <tr><td>r_2</td><td>r_2</td><td>0</td><td>e_2</td><td>0</td></tr> </table>	\cdot	e_1	e_2	r_1	r_2	e_1	e_1	0	0	0	e_2	0	e_2	0	0	r_1	0	r_1	0	e_1	r_2	r_2	0	e_2	0	21	(1,11,17,7,1)
\cdot	e_1	e_2	r_1	r_2																									
e_1	e_1	0	0	0																									
e_2	0	e_2	0	0																									
r_1	0	r_1	0	e_1																									
r_2	r_2	0	e_2	0																									
8	r_1, r_2, a, a^2	<table> <tr><td>\cdot</td><td>r_1</td><td>r_2</td><td>a</td><td>a^2</td></tr> <tr><td>r_1</td><td>0</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>r_2</td><td>0</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>a</td><td>r_2</td><td>r_1+r_2</td><td>a^2</td><td>$a+a^2$</td></tr> <tr><td>a^2</td><td>r_1+r_2</td><td>r_1</td><td>$a+a^2$</td><td>a</td></tr> </table>	\cdot	r_1	r_2	a	a^2	r_1	0	0	0	0	r_2	0	0	0	0	a	r_2	r_1+r_2	a^2	$a+a^2$	a^2	r_1+r_2	r_1	$a+a^2$	a	7	(1,7,11,1,1)
\cdot	r_1	r_2	a	a^2																									
r_1	0	0	0	0																									
r_2	0	0	0	0																									
a	r_2	r_1+r_2	a^2	$a+a^2$																									
a^2	r_1+r_2	r_1	$a+a^2$	a																									
9	r_1, r_2, a, a^2	<table> <tr><td>\cdot</td><td>r_1</td><td>r_2</td><td>a</td><td>a^2</td></tr> <tr><td>r_1</td><td>0</td><td>0</td><td>r_2</td><td>r_1+r_2</td></tr> <tr><td>r_2</td><td>0</td><td>0</td><td>r_1+r_2</td><td>r_1</td></tr> <tr><td>a</td><td>0</td><td>0</td><td>a^2</td><td>$a+a^2$</td></tr> <tr><td>a^2</td><td>0</td><td>0</td><td>$a+a^2$</td><td>a</td></tr> </table>	\cdot	r_1	r_2	a	a^2	r_1	0	0	r_2	r_1+r_2	r_2	0	0	r_1+r_2	r_1	a	0	0	a^2	$a+a^2$	a^2	0	0	$a+a^2$	a	7	(1,7,11,1,1)
\cdot	r_1	r_2	a	a^2																									
r_1	0	0	r_2	r_1+r_2																									
r_2	0	0	r_1+r_2	r_1																									
a	0	0	a^2	$a+a^2$																									
a^2	0	0	$a+a^2$	a																									

ГЛАВА I. Теоретические основы

1. Основные алгебраические структуры

Понятие группы

Определение 1. Группой называется множество G , на котором определена бинарная алгебраическая операция \circ удовлетворяющая следующим условиям:

- 1) $(\forall a, b, c \in G)(a \circ (b \circ c) = (a \circ b) \circ c)$ (ассоциативность);
- 2) $(\exists e \in G)(\forall a \in G)(a \circ e = e \circ a = a)$ (нейтральный элемент);
- 3) $(\forall a \in G)(\exists a' \in G)(a \circ a' = a' \circ a = e)$ (симметричный элемент).

Замечание 1. Если операция \circ является умножением, то будем обозначать ее точкой и пускать точку в тех случаях, когда ясно, что рассматривается произведение (то есть $a \cdot b = ab$). Симметричный элемент a' будем называть обратным, и будем обозначать a^{-1} (то есть $a' = a^{-1}$). Если операция \circ является сложением, то группу будем называть аддитивной, нейтральный элемент e будем обозначать нулем (то есть $e = 0$). Симметричный элемент a' будем называть противоположным, и будем обозначать $-a$ (то есть $a' = -a$).

Примеры групп.

а) Аддитивные группы.

- 1) $G = (Z, +)$ – группа целых чисел;
- 2) $G = (R, +)$ – группа действительных чисел;
- 3) $G = (V, +)$ – группа V – множество геометрических векторов в трехмерном евклидовом пространстве;
- 4) $G = (\bar{Z}, +)$, где $\bar{Z} = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4} \}$ – это классы целых чисел по модулю 5.

Сложение определяется по следующей формуле:

$$\bar{a} + \bar{b} = \overline{a + b}.$$

Таблица сложения:

Таблица №1

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

б) Мультипликативные группы.

- 1) $G = (Q \setminus \{0\}, \cdot)$ – группа ненулевых рациональных чисел;
- 2) $G = (M_n(R), \cdot)$ – группа невырожденных матриц порядка n ;
- 3) $G = (\bar{Z}, +)$, где $\bar{Z} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ – классы ненулевых целых чисел по модулю 5.

Умножение определяется по следующей формуле:

$$\bar{a} \cdot \bar{b} = \overline{a \cdot b}.$$

Таблица умножения:

Таблица №2

\cdot	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Основные свойства групп

Свойство 1. В любой группе нейтральный элемент единственен.

Доказательство. Пусть e_1, e_2 – два нейтральных элемента в группе G .

Тогда:

$$e_1 = e_1 \circ e_2 = e_2.$$

Свойство 2. В любой группе симметричный элемент единственен для каждого элемента.

Доказательство. Пусть a_1' и a_2' - симметричные элементы для элемента a в группе G . Тогда:

$$a_1' = a_1' \circ e = a_1' \circ (a \circ a_2') = (a_1' \circ a) \circ a_2' = e \circ a_2' = a_2'$$

Свойство 3. В любой группе G для любых элементов a и b , уравнения: $a \circ x = b$, $y \circ a = b$ имеют и притом единственные решения: $x = a' \circ b$, $y = b \circ a'$ соответственно.

Доказательство.

Существование:

$$1) a \circ (a' \circ b) = (a \circ a') \circ b = e \circ b = b;$$

$$2) (b \circ a') \circ a = b \circ (a' \circ a) = b \circ e = b.$$

Единственность:

Пусть $c \in G$ и $a \circ c = b$. Тогда:

$$a' \circ (a \circ c) = a' \circ b,$$

$$(a' \circ a) \circ c = a' \circ b,$$

$$e \circ c = a' \circ b,$$

$$c = a' \circ b.$$

Единственность решения второго уравнения доказывается аналогично.

Свойство 4. Правило сокращения.

$$(\forall a, b, c \in G)(a \circ b = a \circ c \Rightarrow b = c).$$

Доказательство.

$$\begin{aligned} b &= e \circ b = (a' \circ a) \circ b = a' \circ (a \circ b) = a' \circ (a \circ c) = \\ &= (a' \circ a) \circ c = e \circ c = c. \end{aligned}$$

Понятие подгруппы

Определение 2. Подмножество S группы (G, \cdot) называется подгруппой группы G , если множество S является группой относительно операции \cdot определенной на G .

Примеры подгрупп.

- 1) $G = (Q \setminus \{0\}, \cdot)$ – группа ненулевых рациональных чисел;
 $S = Q^+$ – множество положительных, рациональных чисел, будет являться подгруппой для группы G ;
- 2) $G = (Q \setminus \{0\}, \cdot)$ – группа ненулевых рациональных чисел;
 $S = \{2^z | z \in Z\}$ – множество целых степеней числа 2, будет являться подгруппой для группы G .

Свойства подгрупп: Пусть (G, \cdot) – группа и (S, \cdot) – ее подгруппа.

Свойство 1. Любая подгруппа – непустое множество, так как содержит нейтральный элемент.

Свойство 2. Единичный элемент любой подгруппы равен единичному элементу самой группы.

Доказательство: Пусть e – единичный элемент группы G , e_1 – единичный элемент подгруппы S . Пусть $a \in S$. Тогда по правилу сокращения:

$$a \cdot e_1 = a = a \cdot e \Rightarrow e_1 = e$$

Свойство 3. Если S_1 и S_2 – две подгруппы группы G , то их пересечение есть непустое множество, то есть $S_1 \cap S_2 \neq \emptyset$.

Свойство 4. В любой группе содержится, по крайней мере, две подгруппы: $E = \{e\}$ – единичная подгруппа и сама группа G .

Признаки подгруппы.

Теорема 1. (Первый признак подгруппы)

Непустое подмножество S , группы (G, \cdot) тогда и только тогда является подгруппой в группе G , когда выполняются два условия:

- 1) $(\forall a, b \in S)(ab \in S)$;
- 2) $(\forall a \in S)(a^{-1} \in S)$.

Доказательство.

Необходимость. Пусть S – подгруппа группы G . Докажем, что выполняются условия 1) и 2). Условие 1) выполнено, так как в группе S и G одна и та же операция умножение. По свойству групп элемент a^{-1} – единственен, значит $a^{-1} \in S$.

Достаточность. Пусть выполнено условие 1) и 2). Докажем, что S – подгруппа в группе G . Из условия 1) следует, что умножение, определенное на группе G , определено и в S .

1) Умножение ассоциативно в S .

2) Так как $S \neq \emptyset$, то существует $a \in S$. Тогда $a^{-1} \in S$ и потому $a \cdot a^{-1} \in S$ и $a \cdot a^{-1} = e \Rightarrow e \in S$.

Теорема 2. (Второй признак подгруппы)

Пусть (G, \cdot) – мультипликативная группа и S – непустое подмножество в группе G . Подмножество S тогда и только тогда является подгруппой в группе G , когда выполнено условие: $(\forall a, b \in S)(a \cdot b^{-1} \in S)$.

Доказательство.

Необходимость. Пусть S – подгруппа и $a, b \in S$. Тогда $b^{-1} \in S$. Значит $a \cdot b^{-1} \in S$.

Достаточность. Пусть $(\forall a, b \in S)(a \cdot b^{-1} \in S)$. Доказать что S – подгруппа. По условию S – непустое подмножество. Пусть $a \in S$. По условию $a \cdot a^{-1} \in S \Rightarrow e \in S$. Применим условие к элементам e и a . Тогда $(\forall a \in S) e \cdot a^{-1} = a^{-1} \in S$. Значит условие 2) в первом признаке подгруппы выполнено. Пусть $a, b \in S$. Тогда $ab^{-1} \in S$. Значит $ab = a(b^{-1})^{-1} \in S$. Таким образом, S – подгруппа.

Понятие кольца

Определение 3. Ассоциативным кольцом называется множество K , с определенными на нем двумя бинарными, алгебраическими операциями $+$, \cdot удовлетворяющее следующим условиям:

- 1) $(\forall a, b, c \in K)(a + (b + c)) = ((a + b) + c)$;
- 2) $(\forall a, b \in K)(a + b = b + a)$;
- 3) $(\exists 0 \in K)(\forall a \in K)(a + 0 = a)$;
- 4) $(\forall a \in K)(\exists (-a) \in K)(a + (-a) = 0)$;
- 5) $(\forall a \in K)(a(bc) = (ab)c)$;
- 6) $(\forall a, b, c \in K)(a(b + c) = ab + ac \wedge (b + c)a = ba + ca)$.

Если умножение в кольце K – коммутативно, то K называется коммутативным кольцом. Если относительно умножения существует нейтральный элемент в кольце K , то K называется кольцом единиц. Коммутативное, ассоциативное кольцо с единицей будем называть кольцом с делением, если в нем для каждого ненулевого элемента существует обратный элемент.

Примеры колец:

Таблица № 3

Кольца	Коммутативное	С единицей	С делением
$(\mathbb{Z}, +, \cdot)$	+	+	–
$(\mathbb{Q}, +, \cdot)$	+	+	+
$(\mathbb{R}, +, \cdot)$	+	+	+
$(\mathbb{C}, +, \cdot)$	+	+	+
$(\mathbb{R}[x], +, \cdot)$	+	+	–

Свойства колец.

Пусть $(K, +, \cdot)$ – произвольное ассоциативное кольцо.

Свойство 1. $(K, +)$ – абелева группа;

Свойство 2. (K, \cdot) – полугруппа;

Свойство 3. $(\forall a \in R)(0 \cdot a = a \cdot 0 = 0)$;

Доказательство: $0 + 0 = 0 \Rightarrow a(0 + 0) = a \cdot 0 + 0 \cdot a = a \cdot 0 \Rightarrow$
 $a \cdot 0 = 0$

Второе равенство доказывается аналогично.

Свойство 4. $(\forall a, b \in K)(a(-b) = (-a)b = -ab)$;

Доказательство: $0 = a \cdot 0 = a(b - b) = a(b + (-b)) = ab + a(-b) \Rightarrow$
 $a(-b) = -ab.$

Второе равенство доказывается аналогично.

Свойство 5. $(\forall a, b, c \in K)(a(b - c) = ab - ac \wedge (b - c)a = ba - ca).$

Доказательство: $a(b - c) = a(b + (-c)) = ab + (-ac) = ab - ac.$

Второе равенство доказывается аналогично.

Понятие подкольца

Определение 4. Подмножество S , кольца K , называется подкольцом, если S является кольцом относительно операций $+$, \cdot определенных в K .

Примеры подколец:

- 1) S – Подмножество четных чисел, является подкольцом в кольце Z целых чисел.
- 2) S – Подмножество в кольце многочленов $R[x]$, в которых x присутствует в четной степени.

Признак подкольца.

Теорема 3. Непустое подмножество S кольца $(K, +, \cdot)$ является подкольцом в K тогда и только тогда, когда выполнены следующие условия:

- 1) $(\forall a, b \in S)((a - b) \in S)$;
- 2) $(\forall a, b \in S)(ab \in S)$.

Доказательство:

Необходимость. S – Подкольцо в K . Тогда S замкнуто относительно умножения, а значит, выполнено условие 2), $(S, +)$ является подгруппой в $(K, +)$ и поэтому выполняется условие 1).

Достаточность. Пусть выполнено условие 1) и 2) из этого вытекает $(S, +)$ является подгруппой в $(K, +)$, это значит сложение определено и аксиомы кольца 1) – 4) выполнены. Из выполнимости условия 2) следует, что умножение определено на S и значит, выполняется условие 5. Таким образом, S – подкольцо.

Понятие поля

Определение 5. Множество F содержащее не менее двух элементов называется полем, если на нем определены две бинарные, алгебраические операции $+$, \cdot удовлетворяющие следующим условиям:

- 1) $(\forall a, b, c \in F)(a + (b + c)) = ((a + b) + c)$;
- 2) $(\forall a, b \in F)(a + b = b + a)$;
- 3) $(\exists 0 \in F)(\forall a \in F)(a + 0 = a)$;

- 4) $(\forall a \in F)(\exists (-a) \in F)(a + (-a) = 0);$
- 5) $(\forall a, b, c \in F)(a(b \cdot c) = (ab)c);$
- 6) $(\forall a, b \in F)(ab = ba);$
- 7) $(\exists 1 \in F)(\forall a \in F)(1 \cdot a = a);$
- 8) $(\forall a \in F \setminus \{0\})(\exists a^{-1} \in F)(a \cdot a^{-1} = 1);$
- 9) $(\forall a, b, c \in K)(a(b + c) = ab + ac).$

Примеры полей

- 1) \mathbb{Q} – поле рациональных чисел;
- 2) \mathbb{R} – поле действительных чисел;
- 3) \mathbb{C} – поле комплексных чисел;
- 4) $K = \{0, 1\}$. Сложение и умножение задается следующими таблицами:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Свойства полей

Пусть $F = (F, +, \cdot)$ – поле.

Свойство 1. $(F, +)$ – абелева группа;

Свойство 2. $(F \setminus \{0\}, \cdot)$ – мультипликативная группа;

Свойство 3. $(F, +, \cdot)$ – коммутативное кольцо с делением и единицей.

Понятие подполя

Определение 6. Подмножество S поля F называется подполем, если S – поле относительно операций $+, \cdot$ определенных в F .

Примеры подполей.

- 1) \mathbb{Q} – поле рациональных чисел, является подполем поля действительных чисел \mathbb{R} ;
- 2) \mathbb{R} – поле действительных чисел, является подполем поля комплексных чисел \mathbb{C} ;

- 3) Q – поле рациональных чисел, является подполем поля комплексных чисел C .

Признак подполя.

Теорема 4. Подмножество S , содержащее не менее двух элементов, тогда и только тогда является подполем в F , когда выполнены следующие условия:

- 1) $(\forall a, b \in S)((a - b) \in S)$;
- 2) $(\forall a, b \in S)(ab \in S)$;
- 3) $(\forall a \in S \setminus \{0\})(a^{-1} \in S)$.

Доказательство.

Необходимость. Пусть S – подполе. Тогда S является полем и потому условия 1) – 3) выполнены.

Достаточность. Пусть выполнены условия 1) – 3). Из условий 1) и 2) следует, что S – подкольцо в $(F, +, \cdot)$, а значит выполнены аксиомы поля 1) – 4) и условия ассоциативности и дистрибутивности умножения. Из выполнимости условия 3) следует, существование обратных элементов в S и существование единичного элемента. Значит, аксиома поля 7) выполнена. Аксиома 6) выполняется, так как умножение коммутативно в поле F . Таким образом, S – подполе.

Понятие векторного пространства

Определение 7. Векторным (линейным) пространством над полем P называется множество V с определенными на нем операциями сложения $+$ и умножения элементов из P на элементы из V со значениями в V (то есть $P \times V \Rightarrow V$), удовлетворяющими условиям:

- 1) $(\forall a, b \in V)(a + b = b + a)$;
- 2) $(\forall a, b, c \in V)(a + (b + c) = (a + b) + c)$;
- 3) $(\exists \bar{0} \in V)(\forall a \in V)(a + \bar{0} = a)$;
- 4) $(\forall a \in V)(\exists (-a))(a + (-a) = \bar{0})$;
- 5) $(\forall a \in V)(\forall \alpha, \beta \in P)(\alpha(\beta a) = (\alpha\beta)a)$;
- 6) $(\forall a, b \in V)(\forall \alpha \in P)(\alpha(a + b) = \alpha a + \alpha b)$;

$$7) (\forall a \in V)(\forall \alpha, \beta \in P)((\alpha + \beta)a = \alpha a + \beta a);$$

$$8) (\forall a \in V)(1 \cdot a = a).$$

Примеры векторных пространств.

1) V_2 – линейное пространство геометрических векторов плоскости;

2) V_3 – линейное пространство геометрических векторов пространства;

Свойства векторных пространств.

Свойство 1. $(\forall a \in V)(0 \cdot a = \bar{0})$.

Свойство 2. $(\forall \alpha \in P)(\alpha \bar{0} = \bar{0})$.

Свойство 3. $(\forall \alpha \in P)(\forall a \in V)(\alpha a = \bar{0} \Leftrightarrow \alpha = 0 \vee a = \bar{0})$.

Свойство 4. $(\forall \alpha \in P)(\forall a \in V)(\alpha(-a) = (-\alpha)a = -\alpha a)$.

Свойство 5. $(\forall \alpha \in P)(\forall a, b \in V)(\alpha(a - b) = \alpha a - \alpha b)$.

Свойство 6. $(\forall \alpha, \beta \in P)(\forall a \in V)((\alpha - \beta)a = \alpha a - \beta a)$.

2. Алгебры над полем

Понятие алгебры

Определение 1. Алгеброй над полем P называется множество A с определенными на нем двумя бинарными, алгебраическими операциями $+$, \cdot и операций умножения элементов из P на элемент из A удовлетворяющее следующим условиям:

1) $(A, +, \cdot)$ – кольцо;

2) $(A, +, \cdot)$ – векторное пространство над P ;

3) $(\forall \alpha \in P)(\forall a, b \in V)(\alpha(ab) = (\alpha a)b = a(\alpha b))$.

Если кольцо $(A, +, \cdot)$ является ассоциативным (коммутативным, с единицей, с делением) то и алгебра A называется ассоциативной (коммутативной, с единицей, с делением) соответственно.

Представим условия 1) – 3) в развернутом виде и получим следующее определение.

Определение 2. Алгеброй над полем P называется множество A с определенными на нем двумя бинарными, алгебраическими операциями $+$, \cdot

и операций умножения элементов из P на элемент из A удовлетворяющее следующим десяти условиям:

- 1) $(\forall a, b, c \in A)((a + b) + c = a + (b + c));$
- 2) $(\forall a, b \in A)(a + b = b + a);$
- 3) $(\exists 0 \in A)(\forall a \in A)(a + 0 = a);$
- 4) $(\forall a \in A)(\exists -a \in A)(a + (-a) = 0);$
- 5) $(\forall a, b, c \in A)(a(b + c) = ab + ac \wedge (a + b)c = ac + bc);$
- 6) $(\forall \alpha, \beta \in P)(\forall a \in A)(\alpha(\beta a) = (\alpha\beta)a);$
- 7) $(\forall \alpha, \beta \in P)(\forall a \in A)((\alpha + \beta)a = \alpha a + \beta a);$
- 8) $(\forall \alpha \in P)(\forall a, b \in A)((\alpha(a + b) = \alpha a + \alpha b);$
- 9) $(\forall a \in A)(1 \cdot a = a);$
- 10) $(\forall \alpha \in P)(\forall a, b \in A)(\alpha(ab) = (\alpha a)b = a(\alpha b)).$

Примеры алгебр.

- 1) $M_n(P)$ – алгебра квадратных матриц порядка n над полем P ;
- 2) $P[x]$ – кольцо многочленов над полем P ;
- 3) V – векторное пространство над P , умножение на V задается следующим образом: $(\forall a, b \in V)(ab = \bar{0})$. Тогда справедливы следующие равенства:
 - 1) $(\forall a, b, c \in V)(a(b + c) = \bar{0} = \bar{0} + \bar{0} = ab + ac);$
 - 2) $(\forall a, b \in V)(\forall \alpha \in P)(\alpha(ab) = \alpha \cdot \bar{0} = \bar{0} = (\alpha a)b = a(\alpha b)).$

Итак, любое векторное пространство можно превратить в алгебру над полем.

Понятие подалгебры

Определение 3. Подмножество S алгебры A над полем P называется подалгеброй алгебры A , если относительно операций, определенных в A , подмножество S является алгеброй над полем P .

Признак подалгебры.

Теорема 1. Непустое подмножество S алгебры A над полем P тогда и только тогда является подалгеброй в A , когда выполнены следующие условия:

- 1) $(\forall a, b \in S)(a - b \in S)$;
- 2) $(\forall a, b \in S)(ab \in S)$;
- 3) $(\forall \alpha \in P)(\forall a \in S)(\alpha a \in S)$.

Доказательство.

Необходимость. Пусть S – подалгебра алгебры A . Тогда очевидно, что условия 1) – 3) выполнены.

Достаточность. Пусть выполнены условия 1) – 3). Тогда из выполнимости условий 1) и 2) следует, что S – подкольцо кольца A , а из выполнимости условий 1) – 3) следует, что S – векторное подпространство пространства A . Аксиома 10) выполняется в S , так как она выполняется в A . Таким образом, S – подалгебра алгебры A .

Предложение 1. Пусть A_i – подалгебра алгебры A над полем P . Тогда $\bigcap A_i$ – подалгебра алгебры A .

Доказательство. Пусть $B = \bigcap A_i$. Так как каждая подалгебра A_i содержит нулевой элемент алгебры A , то $B \neq \emptyset$. Воспользуемся признаком подалгебры. Пусть $a, b \in B$. Тогда $a, b \in A_i$ и поэтому следует $(\forall a, b \in A_i)(a - b \wedge ab \in A_i)$. Следовательно $a - b \wedge ab \in B$. Пусть $\alpha \in P$. Тогда $(\forall \alpha \in P)(\alpha a \in A_i)$ и поэтому $\alpha a \in B$. Таким образом, B – подалгебра алгебры A .

Пусть M – непустое подмножество алгебры A и A_i – подмножество всех подалгебр алгебры A , содержащих M . Тогда согласно предложению 1. $\bigcap A_i$ – подалгебра алгебры A . Тогда подалгебра $\bigcap A_i$ является наименьшей из всех подалгебр, содержащих множество M . Обозначим эту подалгебру через $\langle M \rangle$. Подалгебра $\langle M \rangle$ называется *подалгеброй порожденной множеством M* , а множество M называется *множеством образующих алгебры A* . В случае, когда множество одноэлементное, например $M = \{a\}$, подалгебру $\langle \{a\} \rangle$ будем записывать в виде $\langle a \rangle$ и называть *моногенной* или *однопорожденной* подалгеброй. Если в алгебре A

содержится такой элемент a , что $A = \langle a \rangle$, то будем называть A *моногенной подалгеброй*.

Изоморфизм алгебр.

Определение 4. Пусть A и A' – алгебры над полем P . Изоморфизмом алгебры A на алгебру A' , называется биективное отображение φ , множества A на множество A' удовлетворяющее условиям:

- 1) $(\forall a, b \in A)(\varphi(a + b) = \varphi(a) + \varphi(b))$;
- 2) $(\forall a, b \in A)(\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b))$;
- 3) $(\forall \alpha \in P)(\forall a \in A)(\varphi(\alpha a) = \alpha \varphi(a))$.

Замечание 1. Из условий 1) и 2) следует, что изоморфные алгебры являются изоморфными кольцами, а из условий 1) и 3) следует, что изоморфные алгебры являются изоморфными векторными пространствами. Поэтому изоморфизмы алгебры над полем обладают всеми свойствами изоморфизмов колец и векторных пространств.

Теорема 2. Любая алгебра с единицей ранга n над полем P изоморфна некоторой подалгебре алгебры $M_n(P)$.

Доказательство. Пусть A – алгебра ранга n над полем P . Для любого элемента $a \in A$, определим отображение $\varphi_a: A \rightarrow A$ следующим образом:

$$(\forall x \in A)(\varphi_a(x) = xa)$$

и докажем, что φ_a – линейное отображение.

Действительно,

- 1) $(\forall x, y \in A)(\varphi_a(x + y) = (x + y)a = xa + ya = \varphi_a(x) + \varphi_a(y))$;
- 2) $(\forall x \in A)(\forall \alpha \in P)(\varphi_a(\alpha x) = (\alpha x)a = \alpha(xa) = \alpha \varphi_a(x))$.

Заметим, что $\varphi_{a+b} = \varphi_a + \varphi_b$, $\varphi_{ab} = \varphi_a \cdot \varphi_b$, $\varphi_{\alpha a} = \alpha \varphi_a$.

Обозначим через Φ_n – алгебру всех линейных преобразований векторного пространства A над полем P . Тогда $(\forall a \in A)(\varphi_a \in \Phi_n)$.

Зададим отображение $\psi: A \rightarrow \Phi_n$ по следующему правилу:

$$(\forall a \in A)(\psi(a) = \varphi_a).$$

Докажем что ψ – инъективный гомоморфизм.

В самом деле, пусть $a, b \in A$ и $\psi(a) = \psi(b)$, то есть $\varphi_a = \varphi_b$, значит, $(\forall x \in A)(xa = xb)$. Подставим в это равенство вместо x , единицу алгебры A и получим $a = b$. Значит, ψ – инъективное отображение.

Докажем что ψ – гомоморфизм. Пусть $a, b \in A, \alpha \in P$. Тогда:

- 1) $\psi(a + b) = \varphi_{a+b} = \varphi_a + \varphi_b = \psi(a) + \psi(b);$
- 2) $\psi(ab) = \varphi_{ab} = \varphi_a \cdot \varphi_b = \psi(a) \cdot \psi(b);$
- 3) $\psi(\alpha a) = \varphi_{\alpha a} = \alpha \varphi_a = \alpha \psi(a).$

Следовательно, ψ – гомоморфизм.

Пусть $\psi(A)$ – гомоморфный образ алгебры A . Тогда $\psi(A) \cong A$ и $\psi(A)$ – подалгебра в алгебре Φ_n . Учитывая, что $\Phi_n \cong M_n(P)$, получим утверждение теоремы.

Теорема 3. Пусть A – произвольная алгебра ранга n над полем P . Тогда существует алгебра A^* ранга $n + 1$ с единицей над полем P , содержащая подалгебру, изоморфную алгебре A .

Доказательство. Определим на множестве $A^* = P \times A$ следующие операции:

- 1) $(\forall \alpha, \beta \in P)(\forall a, b \in A^*)((\alpha, a) + (\beta, b) = (\alpha + \beta, a + b));$
- 2) $(\forall \alpha, \beta \in P)(\forall a, b \in A^*)((\alpha, a)(\beta, b) = (\alpha\beta, \alpha b + \beta a + ab));$
- 3) $(\forall \alpha, \beta \in P)(\forall a \in A^*)(\beta(\alpha, a) = (\beta\alpha, \beta a)).$

Очевидно, что $(A^*, +)$ – абелева группа. Проверим выполнимость свойства дистрибутивности умножения относительно сложения:

$$\begin{aligned} (\forall \alpha, \beta, \gamma \in P)(\forall a, b, c \in A^*)((\alpha, a)((\beta, b) + (\gamma, c)) &= (\alpha, a)(\beta + \gamma, b + c) = \\ &= (\alpha(\beta + \gamma), \alpha(b + c) + (\beta + \gamma)a + a(b + c)) = \\ &= (\alpha\beta, \alpha b + \beta a + ab) + (\alpha\gamma, \alpha c + \gamma a + ac) = (\alpha, a)(\beta, b) + (\alpha, a)(\gamma, c) \end{aligned}$$

Следовательно $(A^*, +, \cdot)$ – кольцо. Также, не трудно проверить, что множество A^* относительно условий 1) и 3) образует векторное пространство.

Условие 3) определения 1 также выполнимо в A^* :

$$\begin{aligned} (\forall \alpha, \beta, \gamma \in P)(\forall a, b \in A^*)((\gamma(\alpha, a))(\beta, b) &= (\gamma\alpha\beta, \gamma\alpha b + \beta\gamma a + \gamma\alpha b) = \\ &= \gamma(\alpha\beta, ab + \beta a + ab) = \gamma((\alpha, a)(\beta, b)) = (\alpha, a)(\gamma(\beta, b)). \end{aligned}$$

Таким образом, A^* – алгебра над полем P . Элемент $(1, 0)$, где 1 – единичный элемент поля P , а 0 – нулевой элемент в A , является единицей в алгебре A^* .

Определим размерность алгебры A^* . Пусть e_1, \dots, e_n – базис алгебры A (то есть базис векторного пространства A над полем P). Тогда система векторов $((1, 0), (0, e_1), \dots, (0, e_n))$ алгебры A^* линейно независима над полем P .

Также $(\forall \alpha \in P)(\forall a \in A^*)(\exists \alpha, \alpha_1, \dots, \alpha_n \in P)((\alpha, a) = \alpha(1, 0) + \alpha_1(0, e_1) + \dots + \alpha_n(0, e_n))$. Таким образом, A^* – алгебра ранга $n + 1$.

Рассмотрим отображение $\psi: A \rightarrow A^*$, определенное следующим образом: $(\forall \alpha \in A)(\psi(\alpha) = (0, \alpha))$. Легко заметить, что ψ – инъективное отображение.

Пусть $a, b \in A, \alpha \in P$. Тогда:

- 1) $\psi(a + b) = (0, a + b) = (0, a) + (0, b) = \psi(a) + \psi(b)$;
- 2) $\psi(ab) = (0, ab) = (0, a)(0, b) = \psi(a)\psi(b)$;
- 3) $\psi(\alpha a) = (0, \alpha a) = \alpha(0, a) = \alpha\psi(a)$.

Следовательно, ψ – гомоморфизм, значит алгебра A изоморфна подалгебре $\psi(A)$ алгебры A^* .

3. Решетки

Понятие частично упорядоченного множества

Пусть M – произвольное непустое множество и ρ – бинарное отношение, заданное на нем. Рассмотрим следующие свойства бинарного отношения ρ :

- 1) $(\forall a \in M)(ara)$ (рефлексивность);
- 2) $(\forall a, b \in M)(arb \Rightarrow bra)$ (симметричность);
- 3) $(\forall a \in M)(arb \wedge brs \Rightarrow arcs)$ (транзитивность);
- 4) $(\forall a \in M)(arb \wedge bra \Rightarrow a = b)$ (антисимметричность).

Определение 1. Бинарное отношение, ρ заданное на множестве M , называется отношением частичного порядка, если оно рефлексивно, транзитивно и антисимметрично.

Примеры ч.у. множеств.

- 1) M – любое множество с отношением $=$;
- 2) (N, \leq) – множество натуральных чисел с отношением \leq ;
- 3) $(N, :)$ – множество натуральных чисел с отношением $:$.

Определение 2. Пусть (P, \leq) – ч.у. множество. Будем говорить, что элемент $a \in P$ покрывает элемент $b \in P$, если выполняются следующие условия:

- 1) $b \leq a$;
- 2) $(\forall c \in P)(b \leq c \leq a \Rightarrow c = b \vee c = a)$.

Отношение покрытия позволяет интерпретировать ч.у. множество в виде диаграмм. Для того чтобы изобразить ч.у. множество (P, \leq) в виде диаграммы, примем следующие соглашения:

- 1) различные элементы множества P изображаются различными точками плоскости;
- 2) если $a, b \in P$ и b покрывает a , то точки изображающие эти элементы, соединяются отрезком, причем точка, соответствующая b , располагается выше точки, соответствующей a .

Примеры ч.у. множеств и их диаграмм.

Пример 1. $P = (M, \leq)$, где $M = \{1, 3, 6, 9\}$ (рис 1.);

Пример 2. $S = (M, |)$, где $M = \{1, 2, 3, 6, 9\}$ (рис 2.);



Рис.1

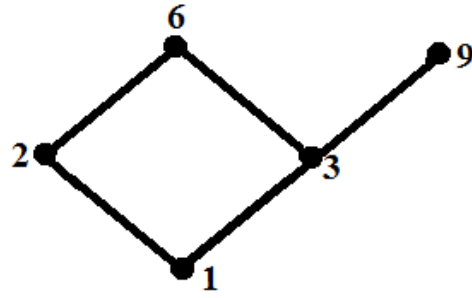


Рис.2

Минимальные и максимальные элементы ч.у. множеств.

Определение 3. Элемент a ч.у. множества (P, \leq) называется наименьшим (наибольшим), если он удовлетворяет условию:

- 1) $(\forall x \in P)(a \leq x)$ (наименьший элемент).
- 2) $(\forall x \in P)(x \leq a)$ (наибольший элемент);

Определение 4. Элемент a ч.у. множества (P, \leq) называется минимальным (максимальным), если он удовлетворяет условию:

- 1) $(\forall x \in P)(x \leq a \Rightarrow x = a)$ (минимальный элемент);
- 2) $(\forall x \in P)(a \leq x \Rightarrow x = a)$ (максимальный элемент).

Замечание 1. Наименьший элемент всегда является минимальным, а наибольший всегда является максимальным.

Числовые характеристики ч.у. множеств.

Определение 5. Подмножество S в ч.у. множестве (P, \leq) называется цепью, если выполняется условие:

$$(\forall x, y \in S)(x \leq y \vee y \leq x)$$

то есть любые 2 элемента сравнимы между собой.

Если $S = \{x_1, \dots, x_n\}$ – конечная цепь, то можно пронумеровать элементы, так что будет выполняться условие:

$$x_1 \leq x_2 \leq \dots \leq x_n$$

Определение 6. Длиной цепи S , состоящей из n – элементов, будем называть число $l(S) = n - 1$.

Определение 7. Длиной ч.у. множества P назовем число n , если в P существует цепь длины n , и длина любой другой цепи в P не больше n .

Определение 8. Подмножество A ч.у. множества P , называется антицепью, если любые два элемента, во множестве A , не сравнимы между собой.

Определение 9. Шириной ч.у. множества P , назовем число n , если в P существует антицепь состоящая из n – элементов и любая другая антицепь содержит не более n – элементов.

Определение 10. Высотой элемента a принадлежащего множеству P с нулевым элементом, называется максимальная из длин цепей между нулевым элементом и элементом a .

Определение 11. Верхней (нижней) границей подмножества S ч.у. множества (P, \leq) , называется элемент $a \in P$, который удовлетворяет условию: $(\forall s \in S)(s \leq a)((\forall s \in S)(a \leq s))$.

Определение 12. Верхней (нижней) гранью подмножества S ч.у.множества (P, \leq) называется наименьший (наибольший) элемент в множестве верхних (нижних) границ подмножества S .

Определение 13. Решеткой (структурой) называется ч.у. множество, в котором каждое двухэлементное подмножество имеет нижнюю и верхнюю грани.

Определение 14. Полной решеткой называется ч.у. множество, в котором каждое подмножество имеет нижнюю и верхнюю грани.

Замечание 2. Любая решетка содержит 0 и 1.

Замечание 3. В любой решетке L каждое конечное подмножество M имеет нижнюю и верхнюю грань.

Приведем определение решетки как алгебры.

Определение 15. Решеткой (структурой) называется непустое множество L с определенными на нем бинарными операциями \wedge и \vee удовлетворяющими следующим условиям:

- 1) $(\forall a \in L)(a \vee a = a, a \wedge a = a)$ (идемпотентность);
- 2) $(\forall a, b \in L)(a \vee b = b \vee a, a \wedge b = b \wedge a)$ (коммутативность);

$$3) (\forall a, b, c \in L)(a \vee (b \vee c) = (a \vee b) \vee c, a \wedge (b \wedge c) = (a \wedge b) \wedge c) \\ (\text{ассоциативность});$$

$$4) (\forall a, b \in L)(a \vee (a \wedge b) = a, a \wedge (a \vee b) = a) \text{ (поглощения)}.$$

Замечание 5. Операции \wedge и \vee используемые в определении решетки, будем называть решеточным объединением и решеточным пересечением соответственно.

Понятие подрешетки

Определение 16. Подрешеткой решетки L называется подмножество S , которое относительно операций \wedge и \vee определенных в L , само является решеткой.

Признак подрешетки.

Теорема 1. Непустое множество S решетки (L, \wedge, \vee) тогда и только тогда является подрешеткой в L , если выполняется условие:

$$(\forall a, b \in S)(a \wedge b \in S, a \vee b \in S).$$

Доказательство. Если S – подрешетка решетки L , то согласно определению 16, S – решетка относительно операций, определенных в L , и поэтому условие теоремы 1, выполнено. Обратно, если выполнено условие теоремы 1, то это значит, что операции \wedge и \vee , определенные в L , определены в S . Свойства 1) – 4) определения 15, выполнимы для этих операций в S , так как они выполнимы для них в L .

ГЛАВА II. Система компьютерной алгебры GAP

1. Общая характеристика

GAP (Groups Algorithms and Programming) – свободно распространяемая и расширяемая система компьютерной алгебры. Является системой компьютерной алгебры, задуманной как инструмент вычислительной теории групп, впоследствии распространившейся на смежные разделы алгебры.

Изначальная разработка системы компьютерной алгебры **GAP** была начата в 1986 году в городе Аахен, Германия. Затем в 1997 году центр разработки переместился в университет города Сент-Эндрюс, Шотландия. В настоящее время **GAP** – это всемирный научный проект, в котором работают специалисты из различных стран мира. Последняя версия **GAP** 4.8.6 была разработана 12 ноября 2016 года.

Основные особенности GAP:

- 1) используется язык программирования, схожий с языком Паскаль;
- 2) применим к основным алгебраическим структурам, таким как: группы, кольца, поля;
- 3) содержит более 4000 пользовательских функций;
- 4) библиотека данных, включая почти все группы, порядок которых не превосходит 2000;
- 5) большое количество прикладных программ;
- 6) обширная документация доступная в различных форматах, а также по сети Internet;
- 7) работает в операционных системах Unix/Linux, а также в Windows, и MacOS;
- 8) работа с процессором типа 386 и выше с ОЗУ от 8 Mb;
- 9) нетребователен к объему памяти на диске.

Установка и запуск системы

Скачать систему можно с сайта: <http://gap-system.org>. Для каждой операционной системы существует своя версия **GAP**. Необходимо выбрать

нужный формат архива и загрузить соответствующий архив. Процедура установки зависит от операционной системы. Полные инструкции по установке в Windows, Linux и Mac OS X доступны в отдельном документе.

Для быстрой проверки установки нужно запустить **GAP**. При успешном запуске системы, на экране появится эмблема **GAP**. Под ней будет напечатана информация о версии системы и установленных компонентах. Командная строка имеет вид: `gap>`.



Для выхода из системы используется команда quit; учитывая то, что каждая команда завершается точкой с запятой и нажатием клавиши Enter .

Алгебраические системы, с которыми работает GAP

Система компьютерной алгебры **GAP** позволяет выполнять вычисления с большими рациональными числами, значения которых ограничивает только доступный объем памяти. Также, система выполняет работу с конечными полями, циклотомическими полями, многочленами от нескольких переменных, рациональными функциями, матрицами и векторами. В том числе доступны различные функции с множествами и списками, комбинаторные и теоретико-числовые функции.

В последующих версиях была доступна возможность работы с векторными пространствами, алгебрами и модулями. Используются алгоритмы для работы с вычислением структуры конечномерных алгебр Ли.

2. Язык программирования GАР

Символы и категории слов

Система **GАР** использует следующие символы: пробел, цифры, буквы, символы новой строки и табуляции и специальные символы:

“	‘	()	*	+	,	–	#
.	/	:	;	<	=	>	~	&
[\]	^	-	{	}	!	

Составленные из символов различные комбинации, называются слова и разделяются на следующие категории:

- 1) целые числа;
- 2) ключевые слова (последовательности букв из нижнего реестра) ;
- 3) строки (последовательности символов, которые обозначены двойными кавычками) ;
- 4) идентификаторы (последовательности букв и цифр, которые содержат не менее одного символа и не являются ключевым словом) ;

Ключевые слова

Ключевыми словами в **GАР** являются: and, else, fi, end, do, elif, function, for, in, if, local, mod, od, not, repeat, or, return, until, then, quit, while, break, rec, continue.

Выражения

Выражениями являются: переменные, целые числа, обращения к функциям, строки, перестановки, списки, функции и записи. Более сложные выражения могут быть составлены с помощью операторов. Различают три вида операторов:

- 1) арифметические операторы: –, +, *, /, ^, mod;
- 2) операторы сравнения: =, <, <>, >=, >, <=, in;

3) логические операторы: and, not, or.

Идентификаторы

Идентификаторы состоят из цифр, букв и символов подчеркивания, при этом должны содержать не менее одного символа или буквы. Примеры идентификаторов: a, x100, hello, HELLO, _10.

3. Команды для вычислений в GAP, используемые в работе

Название команды	Описание
<code>MatAlgebra (GF (n) , m) ;</code>	Построение алгебры матриц порядка m над полем, состоящим из n элементов
<code>Elements (A) ;</code>	Элементы алгебры A
<code>Dimension (A) ;</code>	Размерность алгебры A
<code>M := [] ;</code>	Создание пустого множества M
<code>Size (M) ;</code>	Количество элементов множества M
<code>AddSet (M, m) ;</code>	Добавление элемента m к множеству M
<code>Position (M, m) ;</code>	Положение элемента m в множестве M
<code>Subalgebra (A, [m]) ;</code>	Построение моногенной подалгебры
<code>Intersectset (M, N) ;</code>	Пересечение множества M с множеством N
<code>IsSubsetSet (M, N) ;</code>	Проверка содержатся ли элементы множества N в множестве M
<code>SubtractSet (M, N) ;</code>	Вычитает множество N из множества M , то есть убирает из множества M элементы множества N
<code>UniteSet (M, N) ;</code>	Объединяет элементы множества M с элементами множества N
<code>Sort (M) ;</code>	Упорядочение по возрастанию номеров матриц в массиве M
<u>Условные операторы:</u> <code>if T1 then F1;</code> <code>fi;</code>	Если $T1$ – истина, то следует выполнение команды $F1$

if T1 then F1; elif T2 then F2; fi;	Если $T1$ – истина, то следует выполнение команды $F1$, а если $T2$ – истина, то следует выполнение команды $F2$
if i<j and Subalgebra(A,[El[i]])= Subalgebra(A,[El[j]]) then	Определение матриц, порождающих одну и ту же моногенную подалгебру
<u>Работа с циклами</u> for a in M do Q; od;	Для всех элементов множества M выполняется команда Q
for i in [1..n] do Q; od;	Выполнение команды Q n – раз
<u>Работа с данными</u> Print("N = ",N,"\\n");	Вывод результата на экран
PrintTo("***.dan",M);	Запись данных в файл "***.dan"
Read("***.dan");	Читает файл "***.dan"
quit;	Выход из программы

4. Простейшие программы для вычислений в матричных алгебрах

Программа для нахождения матричной алгебры $M(GF(2))$ и вычисления их квадратов.

Шаг 1. Построим алгебру матриц $M(GF(2))$ и присвоим ей имя A :

```
A:=MatAlgebra(GF(2),2);
```

Шаг 2. Построим массив элементов алгебры A и присвоим ему имя El :

```
El:=Elements(A);
```

Шаг 3. Каждому из 16 элементов массива El присвоим имя m и выведем его на экран:

```
for i in [1..16] do
  Print("m",i,"=",El[i],"\\n");
```

Шаг 4. Не выходя из цикла, открытого на предыдущем шаге, вычислим квадрат матрицы:

```
Print("m", i, "^2=", "m", Position(E1, E1[i]^2), "\n");
```

Шаг 5. Не выходя из цикла, открытого на предыдущем шаге, сравним квадрат матрицы $E1[i]$ с ней самой или с нулевой матрицей и выведем нужную нам информацию на экран. Если $(E1[i]) = E1[i]$, то выведем на экран запись $m = m$, а если $(E1[i]) = 0$, то запишем $m = 0$. Если ни одно из этих равенств не выполнено, то на экран ничего выводить не будем, а перейдем к следующей матрице:

```
if E1[i]^2=E1[i] then
  Print("m", i, ^2=", "m", i, "\n");
else;
  if E1[i]^2=Zero(A) then
    Print("m", i, ^2=", "0", i, "\n");
  fi;
fi;
```

Шаг 6. Завершим цикл, открытый на третьем шаге.

```
od;
```

Результат будет следующим:

```
m1=[ [ 0*Z(2), 0*Z(2) ], [ 0*Z(2), 0*Z(2) ] ]; m1^2=m1;
m2=[ [ 0*Z(2), 0*Z(2) ], [ 0*Z(2), Z(2)^0 ] ]; m2^2=m2;
m3=[ [ 0*Z(2), 0*Z(2) ], [ Z(2)^0, 0*Z(2) ] ]; m3^2=m1;
m4=[ [ 0*Z(2), 0*Z(2) ], [ Z(2)^0, Z(2)^0 ] ]; m4^2=m4;
m5=[ [ 0*Z(2), Z(2)^0 ], [ 0*Z(2), 0*Z(2) ] ]; m5^2=m1;
m6=[ [ 0*Z(2), Z(2)^0 ], [ 0*Z(2), Z(2)^0 ] ]; m6^2=m6;
m7=[ [ 0*Z(2), Z(2)^0 ], [ Z(2)^0, 0*Z(2) ] ]; m7^2=m10;
m8=[ [ 0*Z(2), Z(2)^0 ], [ Z(2)^0, Z(2)^0 ] ]; m8^2=m15;
m9=[ [ Z(2)^0, 0*Z(2) ], [ 0*Z(2), 0*Z(2) ] ]; m9^2=m9;
m10=[ [ Z(2)^0, 0*Z(2) ], [ 0*Z(2), Z(2)^0 ] ]; m10^2=m10;
m11=[ [ Z(2)^0, 0*Z(2) ], [ Z(2)^0, 0*Z(2) ] ]; m11^2=m11;
m12=[ [ Z(2)^0, 0*Z(2) ], [ Z(2)^0, Z(2)^0 ] ]; m12^2=m10;
m13=[ [ Z(2)^0, Z(2)^0 ], [ 0*Z(2), 0*Z(2) ] ]; m13^2=m13;
```

$m14 = [[Z(2)^0, Z(2)^0], [0 \cdot Z(2), Z(2)^0]]$; $m14^2 = m10$;

$m15 = [[Z(2)^0, Z(2)^0], [Z(2)^0, 0 \cdot Z(2)]]$; $m15^2 = m8$;

$m16 = [[Z(2)^0, Z(2)^0], [Z(2)^0, Z(2)^0]]$; $m16^2 = m1$;

Таблица сложения и умножения

Рассмотрим алгоритм построения таблицы сложения. Сначала построим саму алгебру и множество ее элементов:

```
A:=MatAlgebra(GF(2),2);
```

```
El:=Elements(A);
```

Элементы множества El упорядочены особым образом. В соответствии с этим порядком обозначим элементы алгебры $M(GF(2))$ через m_1, m_2, \dots, m_{16} продолжать использовать эти обозначения в новой таблице. Чтобы построить таблицу сложения, нужно каждый элемент $El[i]$ множества El сложить с каждым элементом $El[j]$ этого множества и записать результат в обозначениях m . Следовательно, не нужно запоминать саму сумму $El[i] + El[j]$, а только ее порядковый номер в множестве El . Заготовим массив sum для номеров элементов s :

```
sum:=[];
```

Массив sum будем заполнять следующим образом: сначала создадим в нем первую строку и заполним ее номерами сумм $El[1] + El[j]$ в множестве El для всех номеров j от 1 до 16. Затем создадим в sum вторую строку и заполним ее номерами сумм $El[2] + El[j]$ в множестве El для всех номеров j от 1 до 16. Таким образом заполним все 16 строк массива sum . Соответствующая этому этапу вычислений подпрограмма будет выглядеть следующим образом:

```
for i in [1..16] do
  sum[i]:=[];
  for j in [1..16] do
    sum[i][j]:=Position(El,El[i]+El[j]);
  od; od;
```

Выведем на экран заполненный массив sum :

```
Print("sum:", "\n", sum, "\n");
```

Таблица умножения для элементов алгебры $M(\text{GF}(2), 2)$ получается совершенно аналогично. Поэтому обе таблицы можно получить сразу, добавив к первой программе таблиц умножения в алгебре $M(\text{GF}(2), 2)$ будет выглядеть следующим образом:

```
A:=MatAlgebra(GF(2), 2);
El:=Elements(A);
sum:=[];
prod:=[];
  for i in [1..16] do
    sum[i]:=[];
    prod[i]:=[];
      for j in [1..16] do
        sum[i][j]:=Position(El, El[i]+El[j]);
        prod[i][j]:=Position(El, El[i]*El[j]);
      od; od;
Print("sum:", "\n", sum, "\n", ("prod:", "\n", prod, "\n");
```

После выполнения этой программы результат будет выглядеть следующим образом:

```
sum:
[[ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 ],
 [ 2, 1, 4, 3, 6, 5, 8, 7, 10, 9, 12, 11, 14, 13, 16, 15 ],
 [ 3, 4, 1, 2, 7, 8, 5, 6, 11, 12, 9, 10, 15, 16, 13, 14 ],
 [ 4, 3, 2, 1, 8, 7, 6, 5, 12, 11, 10, 9, 16, 15, 14, 13 ],
 [ 5, 6, 7, 8, 1, 2, 3, 4, 13, 14, 15, 16, 9, 10, 11, 12 ],
 [ 6, 5, 8, 7, 2, 1, 4, 3, 14, 13, 16, 15, 10, 9, 12, 11 ],
 [ 7, 8, 5, 6, 3, 4, 1, 2, 15, 16, 13, 14, 11, 12, 9, 10 ],
 [ 8, 7, 6, 5, 4, 3, 2, 1, 16, 15, 14, 13, 12, 11, 10, 9 ],
 [ 9, 10, 11, 12, 13, 14, 15, 16, 1, 2, 3, 4, 5, 6, 7, 8 ],
 [ 10, 9, 12, 11, 14, 13, 16, 15, 2, 1, 4, 3, 6, 5, 8, 7 ],
```


[11, 12, 9, 10, 15, 16, 13, 14, 3, 4, 1, 2, 7, 8, 5, 6],
 [12, 11, 10, 9, 16, 15, 14, 13, 4, 3, 2, 1, 8, 7, 6, 5],
 [13, 14, 15, 16, 9, 10, 11, 12, 5, 6, 7, 8, 1, 2, 3, 4],
 [14, 13, 16, 15, 10, 9, 12, 11, 6, 5, 8, 7, 2, 1, 4, 3],
 [15, 16, 13, 14, 11, 12, 9, 10, 7, 8, 5, 6, 3, 4, 1, 2],
 [16, 15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1]]

prod:

[[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1],
 [1, 2, 3, 4, 1, 2, 3, 4, 1, 2, 3, 4, 1, 2, 3, 4],
 [1, 1, 1, 1, 2, 2, 2, 2, 3, 3, 3, 3, 4, 4, 4, 4],
 [1, 2, 3, 4, 2, 1, 4, 3, 3, 4, 1, 2, 4, 3, 2, 1],
 [1, 5, 9, 13, 1, 5, 9, 13, 1, 5, 9, 13, 1, 5, 9, 13],
 [1, 6, 11, 16, 1, 6, 11, 16, 1, 6, 11, 16, 1, 6, 11, 16],
 [1, 5, 9, 13, 2, 6, 10, 14, 3, 7, 11, 15, 4, 8, 12, 16],
 [1, 6, 11, 16, 2, 5, 12, 15, 3, 8, 9, 14, 4, 7, 10, 13],
 [1, 1, 1, 1, 5, 5, 5, 5, 9, 9, 9, 9, 13, 13, 13, 13],
 [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16],
 [1, 1, 1, 1, 6, 6, 6, 6, 11, 11, 11, 11, 16, 16, 16, 16],
 [1, 2, 3, 4, 6, 5, 8, 7, 11, 12, 9, 10, 16, 15, 14, 13],
 [1, 5, 9, 13, 5, 1, 13, 9, 9, 13, 1, 5, 13, 9, 5, 1],
 [1, 6, 11, 16, 5, 2, 15, 12, 9, 14, 3, 8, 13, 10, 7, 4],
 [1, 5, 9, 13, 6, 2, 14, 10, 11, 15, 3, 7, 16, 12, 8, 4],
 [1, 6, 11, 16, 6, 1, 16, 11, 11, 16, 1, 6, 16, 11, 6, 1]]

ГЛАВА III. Решеточная характеристика четырехмерных подалгебр алгебры $A=M(GF(2),3)$

1. Понятие типа решетки

В этой главе исследуются решетки четырехмерных подалгебр в алгебре матриц третьего порядка над полем из двух элементов.

Пусть $A = M_3(GF(2))$. Алгебра A – содержит $2^9 = 512$ элементов. Количество подалгебр равно 2102 [7]. К настоящему времени классифицированы все моногенные[8], двухмерные и трехмерные подалгебры алгебры A [9].

Количество четырехмерных подалгебр равно 497[7], но решетки подалгебр четырехмерных алгебр оставались неизученными.

Введем понятие типа решетки, для подалгебры алгебры A .

Определение 1. Пусть S – подалгебра порядка 2^n алгебры $M_3(GF(2))$. Назовем упорядоченную последовательность (m_0, m_1, \dots, m_n) – типом решетки подалгебры алгебры S , если m_i – число подалгебр в S порядка 2^i , где $i = \overline{0, n}$.

Целью исследования является получение классификации четырехмерных подалгебр, по типам их решеток подалгебр. Для каждого отдельного типа решетки, получить классификацию с точностью до изоморфизма самих подалгебр.

Поставленная задача решается с помощью следующего алгоритма:

1) Исходя из пирсовского разложения алгебры, по одному, двум и трем идемпотентным элементам, выбираем базис из четырех элементов. Как правило в качестве базисных элементов берем идемпотентные и нильпотентные элементы индекса 2. И составляем таблицу умножения.

2) Находим в алгебре A , все подалгебры с данной таблицей умножения. Ясно, что все такие подалгебры изоморфны между собой, а значит имеют один и тот же тип решетки. При этом может оказаться, что подалгебры с заданной таблицей умножения не существует.

Данный этап решается на примере следующей программы, реализованной в **GAP**.

Программа нахождения четырехмерных подалгебр		
№	Текст программы	Комментарии
1	<code>EERR:=[];</code>	Создаем массив EERR
2	<code>Sub:=[];b:=0;</code>	Создание массива sub и переменной b
3	<code>NI:=[3, 5, 7, 9, 28, 33, 37, 41, 64, 65, 73, 129, 131, 193, 220, 326, 366, 433, 439, 456, 505];</code>	Массив номеров 2 нильпотентных матриц
4	<code>ID:=[2, 4, 6, 8, 10, 17, 18, 19, 22, 25, 46, 49, 50, 54, 55, 57, 66, 74, 82, 122, 145, 146, 147, 152, 196, 210, 217, 239, 257, 258, 260, 261, 266, 273, 274, 275, 277, 279, 281, 289, 290, 293, 296, 298, 317, 321, 337, 345, 361, 385, 386, 388, 391, 449, 458, 467, 512];</code>	Массив номеров идемпотентных матриц
5	<code>A:=MatAlgebra(GF(2),3);</code>	Построение алгебры матриц третьего порядка над полем GF(2)
6	<code>El:=Elements(A);</code>	Создание массива элементов алгебры A
7	<code>for i in ID do</code>	Начало цикла
8	<code>for j in ID do</code>	Начало цикла
9	<code>for k in NI do</code>	Начало цикла
10	<code>for l in NI do</code>	Начало цикла
11	<code>if j<>i and l<>k and</code>	
12	<code>El[i]*El[j]=El[1] and El[k]*El[i]=El[1] and</code>	Условия
13	<code>El[i]*El[k]=El[1] and El[k]*El[i]=El[1] and</code>	
14	<code>El[i]*El[l]=El[1] and El[l]*El[i]=El[1] and</code>	

15	$El[j] * El[k] = El[l]$ and $El[k] * El[j] = El[l]$ and	
16	$El[j] * El[l] = El[l]$ and $El[l] * El[j] = El[l]$ and	
17	$El[l] * El[k] = El[l]$ and $El[k] * El[l] = El[j]$ then	
18	$B := \text{Subalgebra}(A, [El[i], El[j], El[k], El[l]]);$	Записывает подалгебру алгебры A порожденную элементами $El[i], El[j], El[k], El[l]$ в B
19	$\text{sub} := \text{Elements}(B);$	Кладем в массив sub элементы подалгебры B
20	$\text{AddSet}(\text{Sub}, \text{sub});$	То записываем его в массив Sub
21	if $\text{Size}(\text{Sub}) > b$ then	Сравниваем размер массива Sub с b. Если размер больше
22	$\text{Add}(\text{eerr}, [i, j, k, l]);$	То записываем в массив EERR
23	$b := \text{Size}(\text{Sub});$	Присваиваем b размер массива sub
24	fi; fi;	Конец цикла
25	od; od; od; od;	Конец цикла
26	$\text{Sort}(\text{EERR});$	Упорядочиваем элементы
26	$\text{PrintTo}(\text{"eerr-1.dan"}, \text{"eerr:="}, \text{eerr}, \text{";"}, \text{"\n"}, \text{" eerr ="}, \text{Size}(\text{eerr}), \text{"\n"})$	Печатаем массив EERR в файл eerr-1.dan

3) Для полученного множества изоморфных между собой алгебр определяем их тип решетки подалгебр.

Данный этап решается на примере следующей программы реализованной в **GAP**.

Программа нахождения типа подалгебры		
№	Текст программы	Комментарии
1	<code>tip:=function(a,b,c)</code>	Задаем функцию
2	<code>Local</code>	Создаем локальные переменные
3	<code>A, El, i, j, k, sub, tip, S, s, el, l;</code>	Имена переменных
4	<code>sub:=[];</code>	Задаем пустой массив sub
5	<code>tip:=[];</code>	Задаем пустой массив tip
6	<code>A:=MatAlgebra(GF(2),3);</code>	Создание алгебры матриц
7	<code>El:=Elements(A);</code>	Построение массива элементов
8	<code>S:=Subalgebra(A,[El[a],El[b],El[c]]);</code>	Построение подалгебры
9	<code>for i in S do</code>	Начало цикла
10	<code>for k in S do</code>	Начало цикла
11	<code>for j in S do</code>	Начало цикла
12	<code>s:=Subalgebra(A,[i,j,k]);</code>	Построение подалгебры
13	<code>AddSet(sub,Elements(s));</code>	Построение массива элементов и добавление его в массив sub
14	<code>od; od; od;</code>	Закрытие цикла
15	<code>for l in [1..Size(sub)] do</code>	Начало цикла
16	<code>Add(tip,Size(sub[l]));</code>	Добавление порядка каждого элемента в массив tip
17	<code>od;</code>	Закрытие цикла
18	<code>tip:=Collected(tip);</code>	Считаем количество элементов каждого

		порядка и сохраняем их в tip
19	<code>PrintTo("tip.txt", "a=", "a, ";", " b= ", "b, ";", " c= ", "c, ";", "\n", tip);</code>	Распечатываем результаты в файл tip.txt
20	<code>end;;</code>	Конец функции

4) Если окажется, что ранее были найдены подалгебры с данным типом решетки, то выясняем, получены ли новые подалгебры. Если получены новые, то добавляем их в таблицу.

Данный этап реализуется в **GAP** на примере программы состоящей из массивов подалгебр:

№	Текст программы	Комментарии
1	<code>S1:= [[1, 2, 3, 4, 5, 6, 7, 8, 273, 274, 275, 276, 277, 278, 279, 280],</code> <code>[1, 2, 9, 10, 65, 66, 73, 74, 273, 274, 281, 282, 337, 338, 345, 346],</code> <code>[1, 3, 17, 19, 129, 131, 145, 147, 258, 260, 274, 276, 386, 388, 402, 404],</code> <code>[1, 4, 25, 28, 193, 196, 217, 220, 266, 267, 274, 275, 458, 459, 466, 467],</code> <code>[1, 5, 18, 22, 33, 37, 50, 54, 257, 261, 274, 278, 289, 293, 306, 310],</code> <code>[1, 6, 41, 46, 82, 85, 122, 125, 274, 277, 314, 317, 321, 326, 361, 366],</code> <code>[1, 7, 49, 55, 146, 152, 162, 168, 274, 280, 290, 296, 385, 391, 433, 439],</code> <code>[1, 8, 57, 64, 210, 215, 234, 239, 274, 279, 298, 303, 449, 456, 505, 512],</code> <code>[1, 9, 17, 25, 33, 41, 49, 57, 258, 266, 274, 282,</code>	Массив подалгебры S1

	<p>290, 298, 306, 314],</p> <p>[1, 10, 19, 28, 37, 46, 55, 64, 260, 267, 274, 281, 296, 303, 310, 317],</p> <p>[1, 18, 65, 82, 129, 146, 193, 210, 257, 274, 321, 338, 385, 402, 449, 466],</p> <p>[1, 22, 66, 85, 131, 152, 196, 215, 261, 274, 326, 337, 391, 404, 456, 467],</p> <p>[1, 50, 73, 122, 145, 162, 217, 234, 274, 289, 346, 361, 386, 433, 458, 505],</p> <p>[1, 54, 74, 125, 147, 168, 220, 239, 274, 293, 345, 366, 388, 439, 459, 512]];</p>	
2	<p>S2:=[[1, 2, 3, 4, 5, 6, 7, 8, 273, 274, 275, 276, 277, 278, 279, 280],</p> <p>[1, 2, 9, 10, 65, 66, 73, 74, 273, 274, 281, 282, 337, 338, 345, 346],</p> <p>[1, 3, 17, 19, 129, 131, 145, 147, 258, 260, 274, 276, 386, 388, 402, 404],</p> <p>[1, 4, 25, 28, 193, 196, 217, 220, 266, 267, 274, 275, 458, 459, 466, 467],</p> <p>[1, 5, 18, 22, 33, 37, 50, 54, 257, 261, 274, 278, 289, 293, 306, 310],</p> <p>[1, 6, 41, 46, 82, 85, 122, 125, 274, 277, 314, 317, 321, 326, 361, 366],</p> <p>[1, 7, 49, 55, 146, 152, 162, 168, 274, 280, 290, 296, 385, 391, 433, 439],</p> <p>[1, 8, 57, 64, 210, 215, 234, 239, 274, 279, 298, 303, 449, 456, 505, 512],</p> <p>[1, 9, 17, 25, 33, 41, 49, 57, 258, 266, 274, 282, 290, 298, 306, 314],</p> <p>[1, 10, 19, 28, 37, 46, 55, 64, 260, 267, 274,</p>	<p>Массив подалгебры S2</p>

281, 296, 303, 310, 317], [1, 18, 65, 82, 129, 146, 193, 210, 257, 274, 321, 338, 385, 402, 449, 466], [1, 22, 66, 85, 131, 152, 196, 215, 261, 274, 326, 337, 391, 404, 456, 467], [1, 50, 73, 122, 145, 162, 217, 234, 274, 289, 346, 361, 386, 433, 458, 505], [1, 54, 74, 125, 147, 168, 220, 239, 274, 293, 345, 366, 388, 439, 459, 512]];	
--	--

Далее запускаем программу в **GAP**, и вводим команду: `Intersection(S1,S2);`. Программа проверит данные массивы на изоморфизм подалгебр, содержащихся в них.

5) Если общее количество полученных подалгебр достигает числа 497, то это означает, что все четырехмерные подалгебры классифицированы по типам решетки.

6) Для каждого типа решетки, строим диаграмму решетки подалгебр.

Если для типа решетки существуют несколько попарно не изоморфных подалгебр, то для каждого подмножества попарно изоморфных подалгебр строим диаграмму решетки и выясняем вопрос об изоморфизме самих решеток внутри одного и того же типа.

В результате проведенных исследований найдены все типы решеток четырехмерных подалгебр.

Четырехмерные подалгебры				
№	Тип решетки	Моногенные	Количество подалгебр данного типа	Количество подалгебр данной размерности
1	(1,6,8,4,1)	—	21	497
2	(1,7,11,1,1)	—	14	
3	(1,8,12,6,1)	—	84	
4	(1,9,11,5,1)	—	42	
5	(1,9,13,4,1)	—	84	
6	(1,10,13,3,1)	—	28	

7	(1,11,17,7,1)	–	126	
8	(1,12,18,8,1)	–	84	
9	(1,12,20,9,1)	–	14	

В данной работе были изучены подалгебры типов: (1,8,12,6,1), (1,10,13,3,1), (1,11,17,7,1), (1,7,11,1,1).

Следующие теоремы содержат основные результаты.

Теорема 1. В алгебре матриц $A = M_3(GF(2))$, содержится точно 84 подалгебры, имеющие следующий тип решетки (1,8,12,6,1). Все такие подалгебры, имеют базис: e_1, e_2, r_1, r_2 и следующие таблицы умножения:

Таблица №1

\cdot	e_1	e_2	r_1	r_2
e_1	e_1	0	r_1	r_2
e_2	0	e_2	0	0
r_1	r_1	0	0	0
r_2	0	r_2	0	0

Таблица №2

\cdot	e_1	e_2	r_1	r_2
e_1	e_1	0	r_1	0
e_2	0	e_2	0	r_2
r_1	r_1	r_2	0	0
r_2	0	0	0	0

Доказательство проведено с помощью следующей программы:

Программа №1		
№	Текст программы	Комментарии
1	$EERR := [] ;$	Создаем массив EERR
2	$Sub := [] ; b := 0 ;$	Создание массива sub и переменной b

3	NI:=[3, 5, 7, 9, 28, 33, 37, 41, 64, 65, 73, 129, 131, 193, 220, 326, 366, 433, 439, 456, 505];	Массив номеров нильпотентных матриц 2
4	ID:=[2, 4, 6, 8, 10, 17, 18, 19, 22, 25, 46, 49, 50, 54, 55, 57, 66, 74, 82, 122, 145, 146, 147, 152, 196, 210, 217, 239, 257, 258, 260, 261, 266, 273, 274, 275, 277, 279, 281, 289, 290, 293, 296, 298, 317, 321, 337, 345, 361, 385, 386, 388, 391, 449, 458, 467, 512];	Массив номеров идемпотентных матриц
5	A:=MatAlgebra (GF(2),3);	Построение алгебры матриц третьего порядка над полем GF(2)
6	El:=Elements (A);	Создание массива элементов алгебры A
7	for i in ID do	Начало цикла
8	for j in ID do	Начало цикла
9	for k in NI do	Начало цикла
10	for l in NI do	Начало цикла
11	if j<>i and l<>k and	
12	El[i]*El[j]=El[1] and El[j]*El[i]=El[1] and	Условия
13	El[i]*El[k]=El[k] and El[k]*El[i]=El[k] and	
14	El[i]*El[l]=El[1] and El[l]*El[i]=El[1] and	
15	El[j]*El[k]=El[1] and El[k]*El[j]=El[1] and	
16	El[j]*El[l]=El[1] and El[l]*El[j]=El[1] and	
17	El[l]*El[k]=El[1] and El[k]*El[l]=El[1] then	

18	$B := \text{Subalgebra}(A, [El[i], El[j], El[k], El[l]]);$	Записывает подалгебру алгебры A порожденную элементами $El[i], El[j], El[k], El[l]$ в B
19	$sub := \text{Elements}(B);$	Кладем в массив sub элементы подалгебры B
20	$\text{AddSet}(Sub, sub);$	То записываем его в массив Sub
21	$\text{if Size}(Sub) > b \text{ then}$	Сравниваем размер массива Sub с b . Если размер больше
22	$\text{Add}(eerr, [i, j, k, l]);$	То записываем в массив $EERR$
23	$b := \text{Size}(Sub);$	Присваиваем b размер массива sub
24	$\text{fi}; \text{ fi};$	Конец цикла
25	$\text{od}; \text{ od}; \text{ od}; \text{ od};$	Конец цикла
26	$\text{Sort}(EERR);$	Упорядочиваем элементы
26	$\text{PrintTo}("eerr-1.dan", "eerr:=", eerr, ";", "\n", " eerr =", \text{Size}(eerr), "\n")$	Печатаем массив $EERR$ в файл $eerr-1.dan$

Замечание. Приведенная программа строит подалгебру $eerr-1$.

Программа для построения подалгебры $eerr-2$ отличается в строках 12-17:

$eerr-1$	$eerr-2$
$El[i] * El[j] = El[l] \text{ and}$ $El[j] * El[i] = El[l] \text{ and}$	$El[i] * El[j] = El[l] \text{ and}$ $El[j] * El[i] = El[l] \text{ and}$
$El[i] * El[k] = El[k] \text{ and}$ $El[k] * El[i] = El[k] \text{ and}$	$El[i] * El[k] = El[k] \text{ and}$ $El[k] * El[i] = El[k] \text{ and}$
$El[i] * El[l] = El[l] \text{ and}$ $El[l] * El[i] = El[l] \text{ and}$	$El[i] * El[l] = El[l] \text{ and}$ $El[l] * El[i] = El[l] \text{ and}$
$El[j] * El[k] = El[l] \text{ and}$ $El[k] * El[j] = El[l] \text{ and}$	$El[j] * El[k] = El[l] \text{ and}$ $El[k] * El[j] = El[l] \text{ and}$
$El[j] * El[l] = El[l] \text{ and}$	$El[j] * El[l] = El[l] \text{ and}$

$E_l[l] * E_l[j] = E_l[l] \text{ and}$	$E_l[l] * E_l[j] = E_l[l] \text{ and}$
$E_l[l] * E_l[k] = E_l[l] \text{ and}$	$E_l[l] * E_l[k] = E_l[l] \text{ and}$
$E_l[k] * E_l[l] = E_l[l] \text{ then}$	$E_l[k] * E_l[l] = E_l[l] \text{ then}$

Результатами программ являются массивы номеров четверок базисных элементов.

$eerr-1 := [[18, 257, 3, 5], [18, 257, 9, 33], [18, 257, 28, 37], [22, 261, 41, 33], [22, 261, 64, 37], [50, 289, 7, 5], [82, 321, 9, 41], [82, 321, 131, 326], [82, 321, 220, 366], [122, 361, 439, 366], [122, 361, 456, 326], [146, 385, 3, 7], [146, 385, 73, 433], [146, 385, 220, 439], [152, 391, 366, 439], [152, 391, 505, 433], [210, 449, 28, 64], [210, 449, 73, 505], [210, 449, 131, 456], [239, 512, 326, 456], [239, 512, 433, 505], [258, 17, 5, 3], [258, 17, 65, 129], [258, 17, 326, 131], [260, 19, 193, 129], [260, 19, 456, 131], [266, 25, 37, 28], [266, 25, 65, 193], [266, 25, 366, 220], [273, 2, 33, 9], [273, 2, 129, 65], [273, 2, 433, 73], [275, 4, 129, 193], [275, 4, 439, 220], [277, 6, 33, 41], [279, 8, 37, 64], [281, 10, 193, 65], [281, 10, 505, 73], [290, 49, 5, 7], [337, 66, 41, 9], [386, 145, 7, 3], [458, 217, 64, 28]];$

$|eerr-1|=42$

$eerr-2 := [[18, 257, 3, 129], [18, 257, 9, 65], [18, 257, 28, 193], [22, 261, 3, 131], [22, 261, 41, 326], [22, 261, 64, 456], [50, 289, 7, 433], [50, 289, 9, 73], [50, 289, 64, 505], [54, 293, 7, 439], [54, 293, 28, 220], [54, 293, 41, 366], [82, 321, 131, 129], [82, 321, 220, 193], [122, 361, 439, 433], [122, 361, 456, 505], [146, 385, 73, 65], [152, 391, 366, 326], [152, 391, 505, 456], [239, 512, 326, 366], [239, 512, 433, 439], [258, 17, 5, 33], [258, 17, 65, 9], [258, 17, 326, 41], [260, 19, 5, 37], [260, 19, 193, 28], [260, 19, 456, 64], [266, 25, 37, 33], [266, 25, 366, 41], [273, 2, 33, 5], [273, 2, 129, 3], [273, 2, 433, 7], [275, 4, 37, 5], [275, 4, 439, 7], [277, 6, 131, 3], [281, 10, 33, 37], [281, 10, 505, 64], [290, 49, 73, 9], [296, 55, 220, 28], [337, 66, 129, 131], [345, 74, 193, 220], [386, 145, 65, 73]];$

$|eerr-2|=42$

Доказательство следующих теорем осуществляется с помощью программ, аналогичных программе № 1. Отличия этих программ состоят в блоках, задающих умножения в соответствующей алгебре.

Теорема 2. В алгебре матриц $A = M_3(GF(2))$, содержится точно 28 подалгебр имеющих следующий тип решетки (1,10,13,3,1). Все такие подалгебры изоморфны между собой, имеют базис: e_1, e_2, r_1, r_2 и следующую таблицу умножения:

Таблица №3

\cdot	e_1	e_2	r_1	r_2
e_1	e_1	0	r_1	0
e_2	0	e_2	0	r_2
r_1	0	r_1	0	e_1
r_2	r_2	0	e_2	0

Получен результат в виде массива номеров четверок базисных элементов.

eerr:=[[2, 17, 3, 9], [2, 49, 7, 9], [2, 145, 3, 73], [2, 257, 5, 65], [2, 289, 5, 73], [2, 385, 7, 65], [4, 55, 7, 28], [4, 257, 5, 193], [4, 293, 5, 220], [4, 385, 7, 193], [6, 17, 3, 41], [6, 147, 3, 366], [10, 217, 28, 73], [10, 257, 37, 65], [10, 289, 37, 73], [10, 449, 64, 65], [17, 66, 9, 131], [17, 257, 33, 129], [17, 261, 33, 131], [17, 321, 41, 129], [19, 257, 37, 129], [19, 261, 37, 131], [19, 449, 64, 129], [25, 257, 33, 193], [25, 293, 33, 220], [25, 321, 41, 193], [46, 196, 28, 326], [49, 74, 9, 439]];

$$|eerr|=28$$

Теорема 3. В алгебре матриц $A = M_3(GF(2))$, содержится точно 126 подалгебр имеющих следующий тип решетки (1,11,17,7,1). Все такие подалгебры, имеют базис: e_1, e_2, r_1, r_2 и следующие таблицы умножения:

Таблица №4

\cdot	e_1	e_2	r_1	r_2
e_1	e_1	0	r_1	r_2

e_2	0	e_2	0	0
r_1	0	r_1	0	e_1
r_2	0	0	e_2	0

Таблица №5

\cdot	e_1	e_2	r_1	r_2
e_1	e_1	0	0	0
e_2	0	e_2	r_1	0
r_1	r_1	r_2	0	e_1
r_2	0	0	e_2	0

Таблица №6

\cdot	e_1	e_2	r_1	r_2
e_1	e_1	0	0	r_2
e_2	0	e_2	r_1	0
r_1	0	0	0	e_1
r_2	0	0	e_2	0

Таблица №7

\cdot	e_1	e_2	r_1	r_2
e_1	e_1	0	0	0
e_2	0	e_2	0	0
r_1	0	r_1	0	e_1
r_2	r_2	0	e_2	0

Получен результат в виде массивов номеров четверок базисных элементов.

$eerr-1 := [[2, 17, 3, 5], [2, 49, 7, 5], [2, 145, 3, 7], [2, 257, 5, 3], [2, 289, 5, 7], [2, 385, 7, 3], [10, 25, 28, 37], [10, 57, 64, 37], [10, 217, 28, 64], [$

10, 257, 37, 28], [10, 289, 37, 64], [10, 449, 64, 28], [17, 2, 9, 33], [17, 6, 41, 33], [17, 66, 9, 41], [17, 257, 33, 9], [17, 261, 33, 41], [17, 321, 41, 9], [66, 17, 131, 326], [66, 57, 456, 326], [66, 145, 131, 456], [66, 321, 326, 131], [66, 361, 326, 456], [66, 449, 456, 131], [74, 25, 220, 366], [74, 49, 439, 366], [74, 217, 220, 439], [74, 321, 366, 220], [74, 361, 366, 439], [74, 385, 439, 220], [145, 2, 73, 433], [145, 8, 505, 433], [145, 66, 73, 505], [145, 385, 433, 73], [145, 391, 433, 505], [145, 449, 505, 73], [257, 2, 65, 129], [257, 4, 193, 129], [257, 10, 65, 193], [257, 17, 129, 65], [257, 19, 129, 193], [257, 25, 193, 65]];

|eerr-1|=42

eerr-2:=[[2, 17, 9, 65], [2, 49, 9, 73], [2, 145, 73, 65], [2, 257, 65, 9], [2, 289, 73, 9], [2, 385, 65, 73], [4, 19, 28, 193], [4, 55, 28, 220], [4, 147, 220, 193], [4, 257, 193, 28], [4, 293, 220, 28], [4, 385, 193, 220], [6, 17, 41, 326], [6, 49, 41, 366], [6, 147, 366, 326], [6, 261, 326, 41], [6, 293, 366, 41], [6, 391, 326, 366], [8, 19, 64, 456], [8, 55, 64, 505], [8, 145, 505, 456], [8, 261, 456, 64], [8, 289, 505, 64], [8, 391, 456, 505], [17, 2, 3, 129], [17, 6, 3, 131], [17, 66, 131, 129], [17, 257, 129, 3], [17, 261, 131, 3], [17, 321, 129, 131], [49, 2, 7, 433], [49, 6, 7, 439], [49, 74, 439, 433], [49, 289, 433, 7], [49, 293, 439, 7], [49, 361, 433, 439], [257, 2, 5, 33], [257, 4, 5, 37], [257, 10, 37, 33], [257, 17, 33, 5], [257, 19, 37, 5], [257, 25, 33, 37]];

|eerr-2|=42

eerr-3:=[[2, 17, 33, 5], [2, 145, 433, 7], [2, 257, 129, 3], [4, 19, 37, 5], [4, 147, 439, 7], [6, 261, 131, 3], [10, 25, 33, 37], [10, 217, 505, 64], [10, 257, 193, 28], [17, 66, 326, 41], [17, 257, 65, 9], [19, 196, 456, 64], [25, 74, 366, 41], [46, 293, 220, 28], [49, 289, 73, 9], [66, 145, 505, 456], [66, 321, 129, 131], [74, 217, 433, 439], [74, 321, 193, 220], [145, 385, 65, 73], [147, 196, 326, 366]];

|eerr-3|=21

eerr-4:=[[2, 17, 129, 65], [2, 49, 433, 73], [2, 257, 33, 9], [4, 19, 129, 193], [4, 55, 439, 220], [4, 257, 37, 28], [6, 17, 131, 326], [6, 49, 439, 366], [6, 261, 33, 41], [8, 19, 131, 456], [8, 55, 433, 505], [8, 261, 37, 64], [10, 25,

193, 65], [10, 57, 505, 73], [17, 257, 5, 3], [25, 46, 366, 220], [46, 57, 456, 326], [49, 289, 5, 7], [66, 321, 41, 9], [145, 385, 7, 3], [196, 449, 64, 28]];

$$|eerr-4|=21$$

Теорема 4. В алгебре матриц $A = M_3(GF(2))$, содержится точно 14 подалгебр имеющих следующий тип решетки (1,7,11,1,1). Все такие подалгебры, имеют базис: r_1, r_2, a, a^2 и следующие таблицы умножения:

Таблица №8

\cdot	r_1	r_2	a	a^2
r_1	0	0	0	0
r_2	0	0	0	0
a	r_2	$r_1 + r_2$	a^2	$a + a^2$
a^2	$r_1 + r_2$	r_1	$a + a^2$	a

Таблица №9

\cdot	r_1	r_2	a	a^2
r_1	0	0	r_2	$r_1 + r_2$
r_2	0	0	$r_1 + r_2$	r_1
a	0	0	a^2	$a + a^2$
a^2	0	0	$a + a^2$	a

Получен результат в виде массивов номеров троек базисных элементов.

$eerr-1 := [[3, 129, 325], [5, 33, 27], [7, 433, 219], [9, 65, 417], [28, 193, 357], [41, 326, 204], [64, 456, 91]]$;

$$|eerr-1|=7$$

$eerr-2 := [[3, 5, 417], [9, 33, 325], [28, 37, 453], [65, 129, 27], [73, 433, 63], [131, 326, 48], [220, 366, 31]]$;

$$|eerr-2|=7$$

2. Алгоритм построения диаграмм решеток подалгебр

Пусть требуется построить диаграмму решетки подалгебр подалгебры S алгебры A . Алгоритм построения программы состоит из следующих шагов:

1) Создается массив *sub* в котором будут находиться все подалгебры алгебры *S*.

2) Массив *sub* разбивается на 6 подмассивов соответствующих размерностям подалгебр.

3) Создается сама алгебра *A* и массив ее элементов.

4) Выбирается базис подалгебры *S* и строится сама алгебра *S* и массив ее элементов.

5) С помощью нескольких циклов создается все подалгебры алгебры *S* и массивы их элементов распределяются по соответствующим подмассивам в массиве *sub*.

6) Для каждой подалгебры из массива *sub[i]* находятся все подалгебры в массиве *sub[i+1]*, покрывающие данную подалгебру. Если в подмассиве *sub[i+1]* не нашлось ни одной подалгебры покрывающую данную, то ищем покрывающие в подмассиве *sub[i+2]*, и так далее. В результате получаем массив *pokr*, в котором записаны все отношения покрытия для всех подалгебр алгебры *S*.

7) Используя массив *pokr*, строим диаграмму.

Данный алгоритм реализуется с помощью следующей программы:

Программа нахождения покрытия	
<code>pokr:=function(a,b,c,d)</code>	Задание функции
<code>local</code>	Задание переменных
<code>A, E1, i, j, k, sub, tip, S, s, s1, el, l, l1, m, m1, n, n1, i1;</code>	Имена переменных
<code>sub:=[];</code>	Создаем массив <i>sub</i>
<code>for i1 in [1..6] do</code>	Начало цикла
<code>sub[i1]:=[];</code>	Создаем в массиве <i>sub</i> 6 пустых массивов
<code>od;</code>	Конец цикла
<code>pokr:=[];</code>	Создание массива <i>pokr</i>

<code>A:=MatAlgebra(GF(2),3);</code>	Создание алгебры
<code>El:=Elements(A);</code>	Построение массива элементов
<code>S:=Subalgebra(A,[El[a],El[b],El[c]]);</code>	Записывает подалгебру алгебры A порожденную элементами <code>El[a],El[b],El[c], El[d]</code> в S
<code>for i in S do</code>	Начало цикла
<code>for k in S do</code>	Начало цикла
<code>for j in S do</code>	Начало цикла
<code>s1:=Subalgebra(S,[i,k,j];</code>	Записывает подалгебру алгебры S порожденную элементами <code>i,k,j</code> в s1
<code>if Size(s1)=1 then</code>	Проверяем если размер равен 1
<code>AddSet(sub[1], Elements(s1)); fi;</code>	Записываем в 1-й массив и закрываем проверку условия
<code>if Size(s1)=2 then</code>	Проверяем если размер равен 2
<code>AddSet(sub[2], Elements(s1)); fi;</code>	Записываем во 2-й массив и закрываем проверку условия
<code>if Size(s1)=4 then</code>	Проверяем если размер равен 4
<code>AddSet(sub[3], Elements(s1)); fi;</code>	Записываем в 3-й массив и закрываем проверку условия
<code>if Size(s1)=8 then</code>	Проверяем если размер равен 8
<code>AddSet(sub[4], Elements(s1)); fi;</code>	Записываем в 4-й массив и закрываем проверку условия
<code>if Size(s1)=16 then</code>	Проверяем если размер равен 16
<code>AddSet(sub[5], Elements(s1)); fi;</code>	Записываем в 5-й массив и закрываем проверку условия

$4, 5]], [[3, 4], [4, 2]], [[3, 4], [4, 4]], [[3, 5], [4, 2]], [[3, 5], [4, 5]],$
 $[[3, 6], [4, 3]], [[3, 6], [4, 4]], [[3, 6], [4, 5]], [[3, 7], [4, 1]], [[3, 7], [4, 6]],$
 $[[3, 8], [4, 2]], [[3, 8], [4, 6]], [[3, 9], [4, 3]], [[3, 9], [4, 6]],$
 $[[3, 10], [4, 3]], [[3, 11], [4, 4]], [[3, 11], [4, 6]], [[3, 12], [4, 5]],$
 $[[3, 12], [4, 6]], [[4, 1], [5, 1]], [[4, 2], [5, 1]], [[4, 3], [5, 1]], [[4, 4], [5, 1]],$
 $[[4, 5], [5, 1]], [[4, 6], [5, 1]]];$

В данной программе рассматривается подалгебра S , которая содержит 16 элементов и имеет тип $(1, 8, 12, 6, 1)$. Значит, в ней содержится одна нулевая подалгебра, 8 двухэлементных, 12 четырехэлементных, 6 восьмиэлементных и 1 шестнадцатиэлементная подалгебра. Таким образом, все подалгебры в решетке подалгебр алгебры S распределены по пяти уровням. На каждом уровне алгебры имеют двойные номера, например, номер $[3, 2]$ означает, что 3 – номер уровня, а 2 – порядковый номер подалгебры на третьем уровне. Таким образом, запись $[[3, 2], [4, 1]]$ означает, что подалгебра с номером $[3, 2]$ покрывается подалгеброй с номером $[4, 1]$ в решетке подалгебр алгебры S .

С помощью данной программы вычисляется покрытие подалгебры для каждого определяющего соотношения.

3. Построение диаграмм

Используя полученную информацию, строится диаграмма решетки подалгебр алгебры S . Построение осуществляется в несколько этапов:

1. Изобразим подалгебры алгебры S точками (или кружочками).
2. Изобразим отношение покрытия, соединяя покрываемый элемент с покрывающим отрезком.

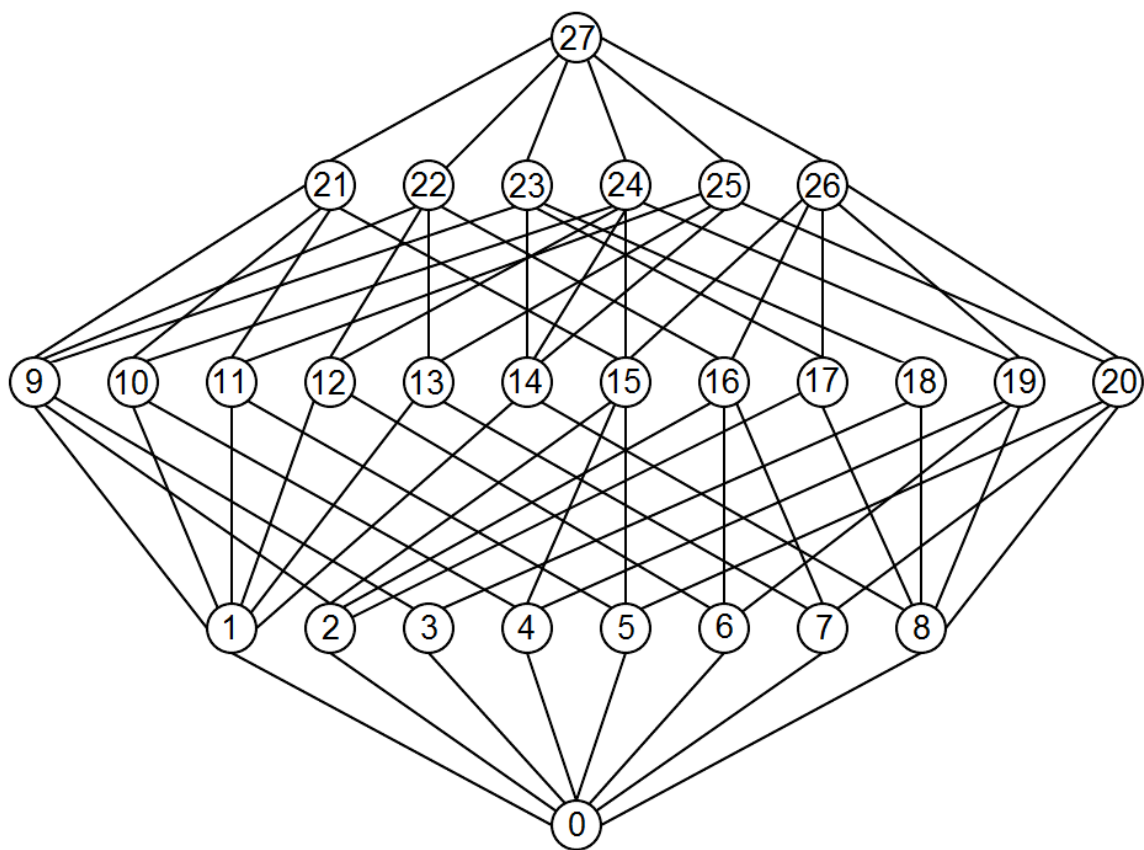


Рисунок 1. Тип (1,8,12,6,1), Таблица №1

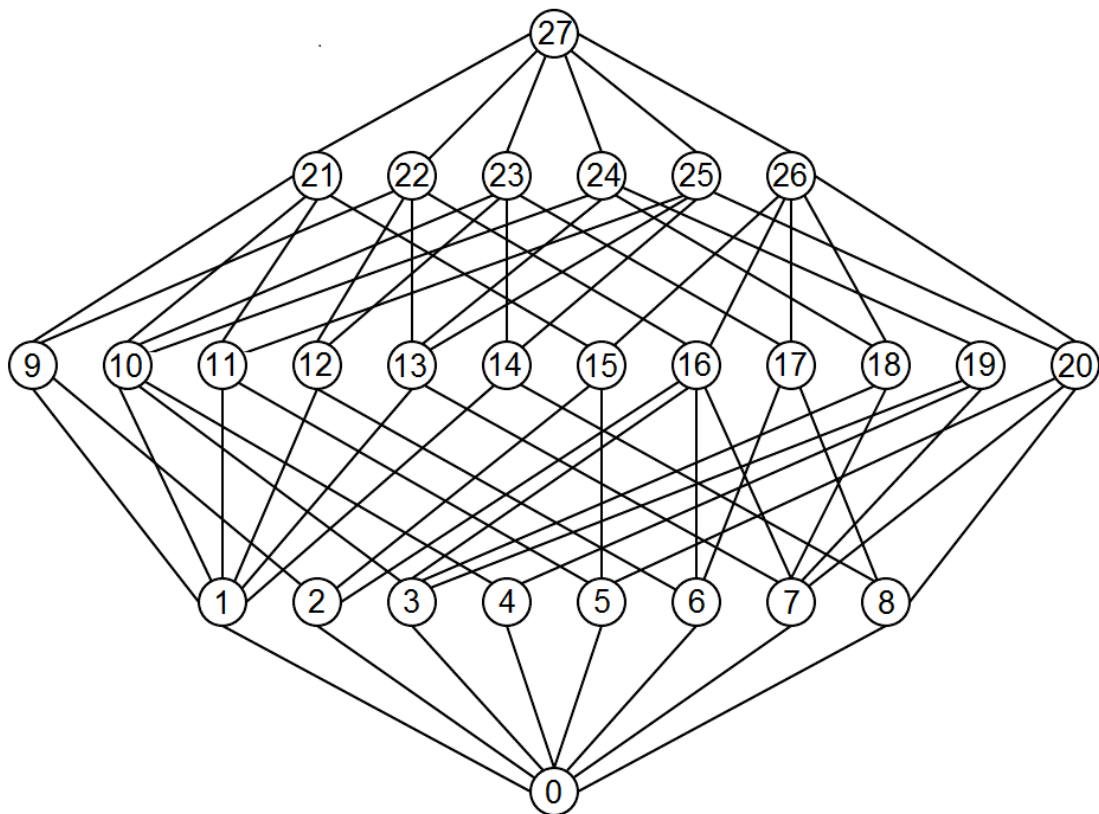


Рисунок 2. Тип (1,8,12,6,1), Таблица №2

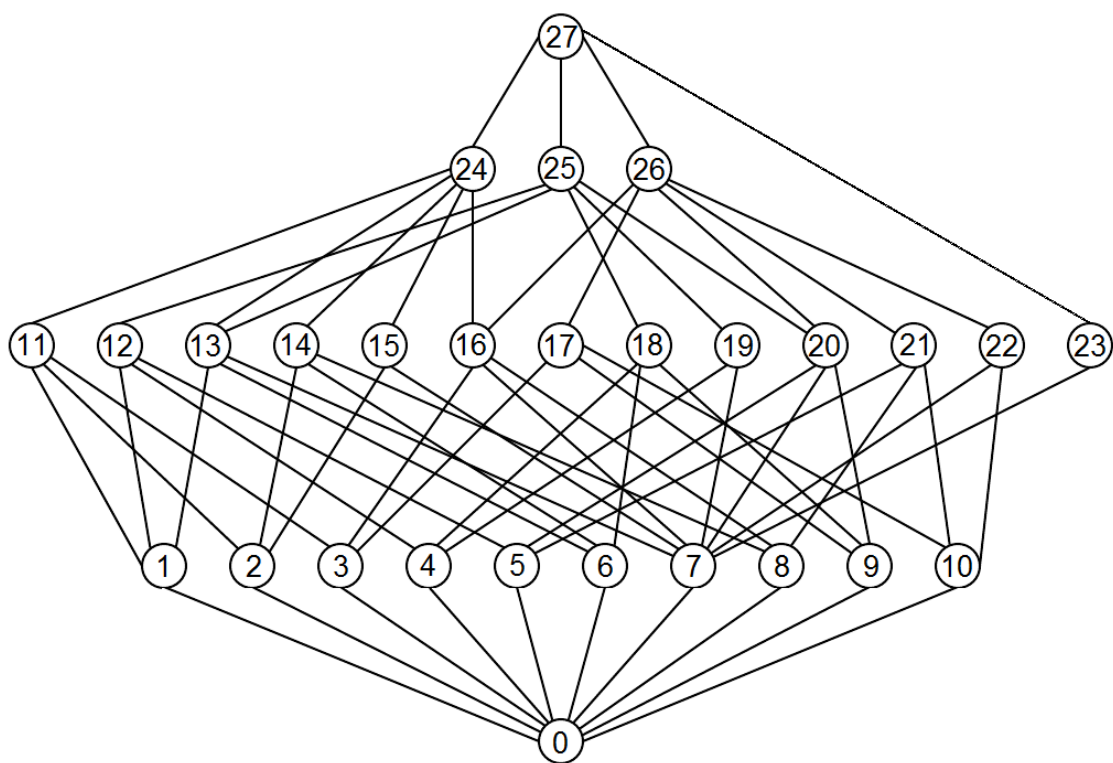


Рисунок 3. Тип (1,10,13,3,1), Таблица №3

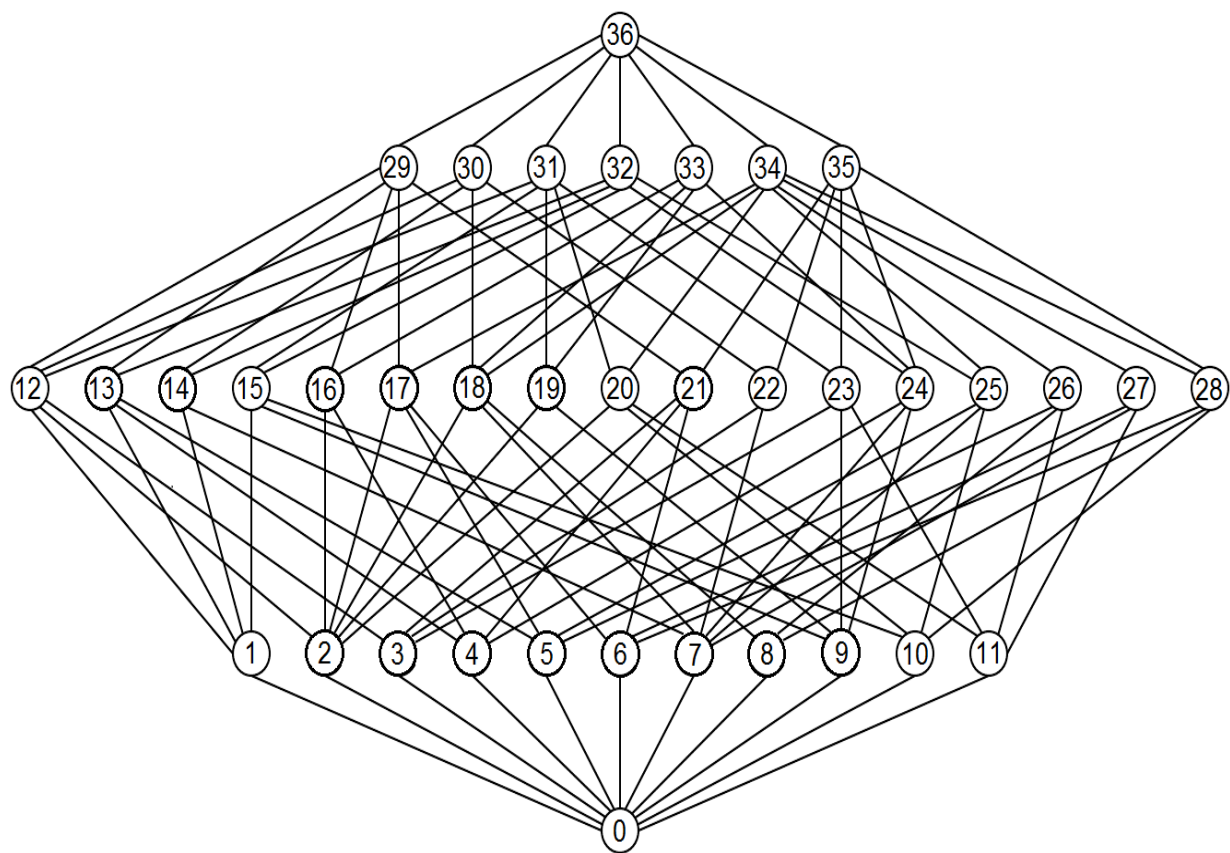


Рисунок 4. Тип (1,11,17,7,1), Таблица №4

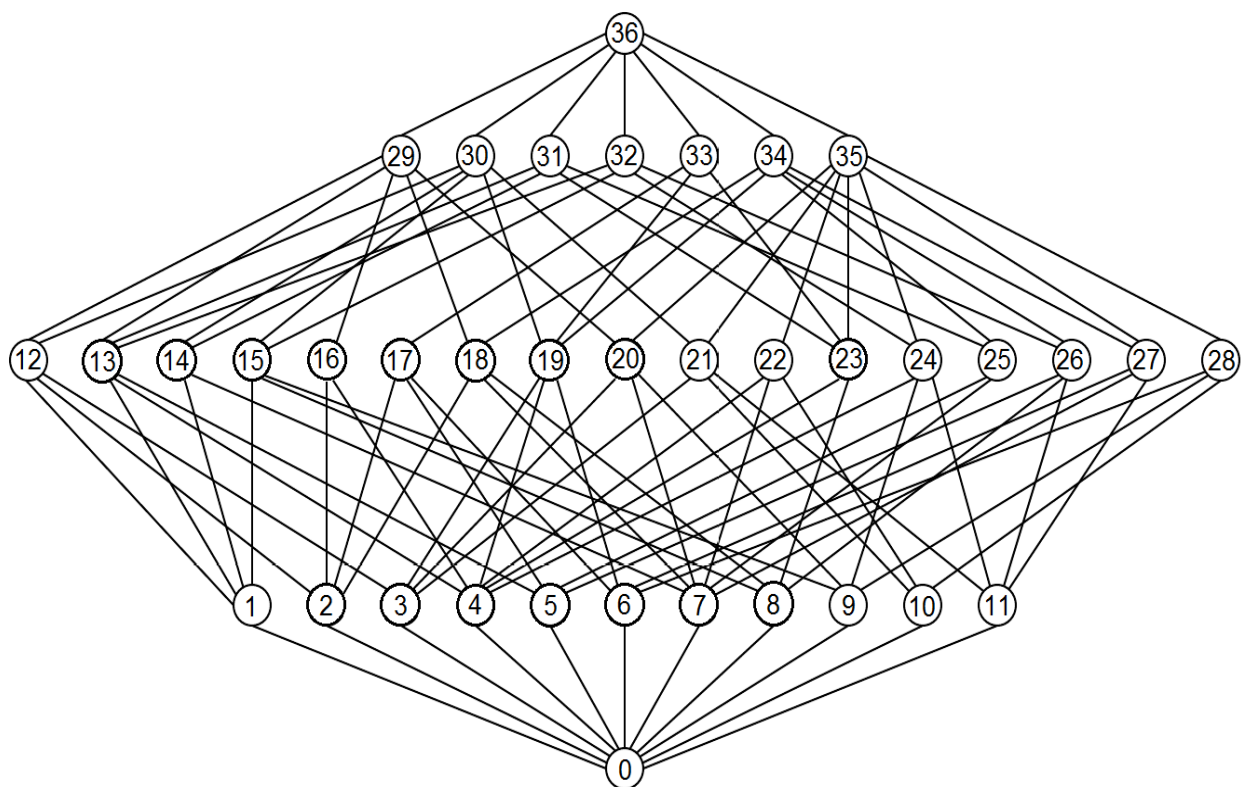


Рисунок 5. Тип (1,11,17,7,1), Таблица №5

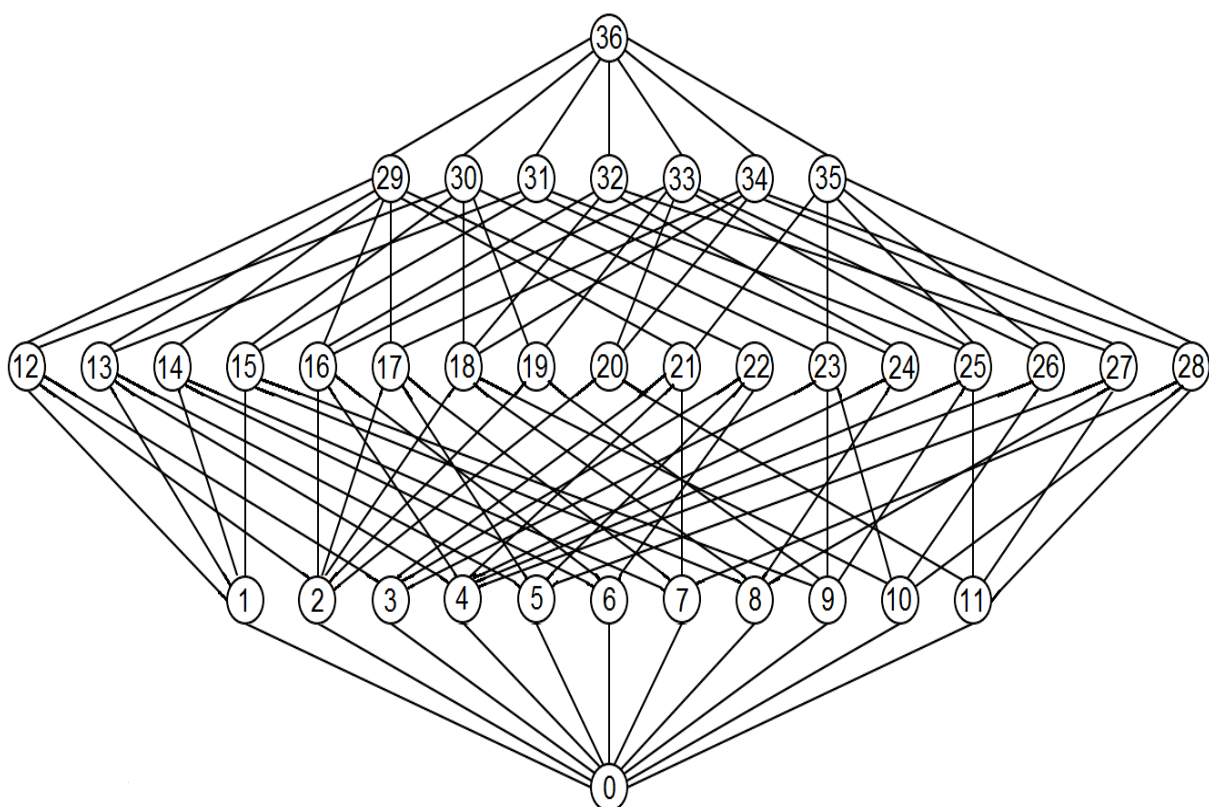


Рисунок 6. Тип (1,11,17,7,1), Таблица №6

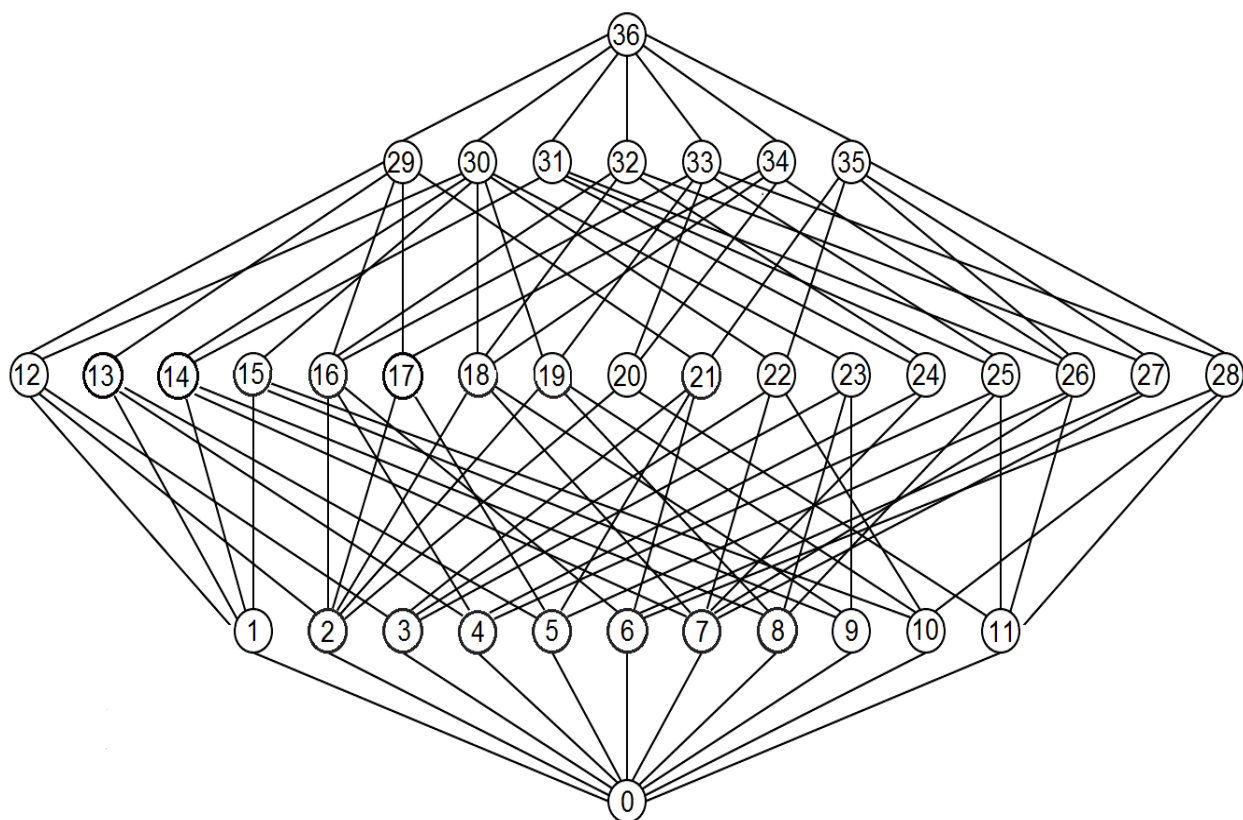


Рисунок 7. Тип (1,11,17,7,1), Таблица №7

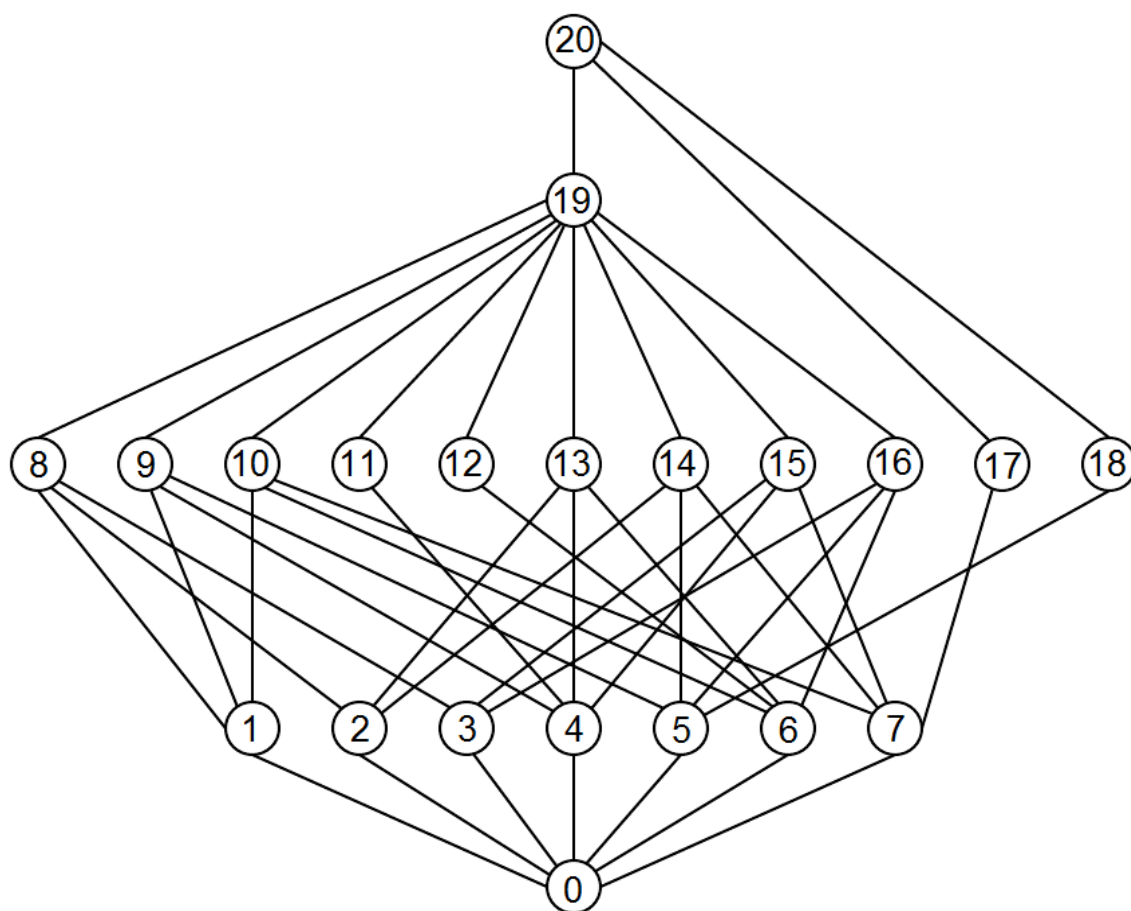


Рисунок 8. Тип (1,7,11,1,1), Таблица №8

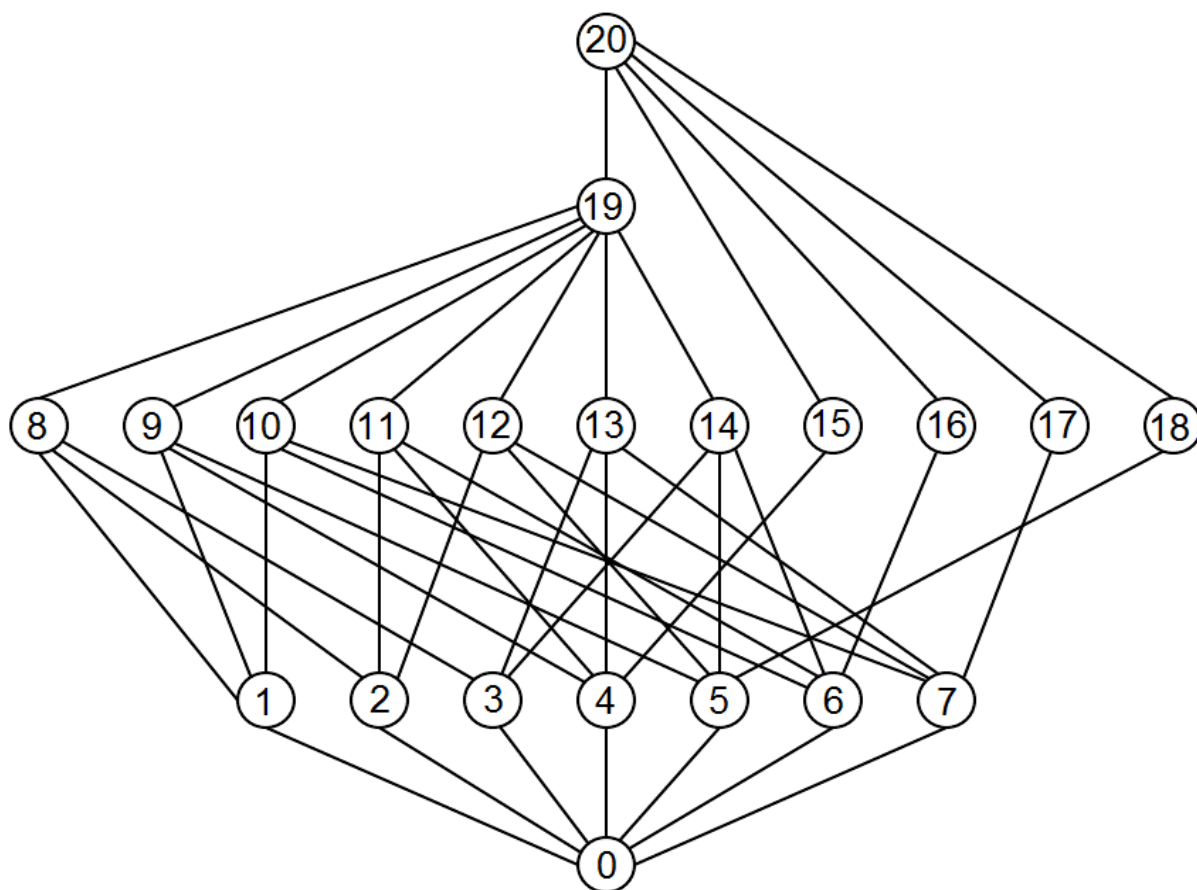


Рисунок 9. Тип (1,7,11,1,1), Таблица №9

Библиографический список

1. Биркгоф, Г. Теория решеток; пер. с англ. В. Н. Салий под ред. Л. А. Скорнякова. – М.: Наука, 1984. – 568 с.
2. Гретцер, Г. Общая теория решеток; пер. с англ. А. Д. Больбота, В. А. Горбунова, В. И. Туманова под ред. Д. М. Смирнова. – М. : Мир, 1982. – 456 с.
3. Калужнин, Л. А. Введение в общую алгебру. – М.: Наука, 1973. – 448 с.
4. Коробков С. С. Введение в теорию решеток: Учеб. пособие по спец. курсу. Урал. гос. пед. ун-т. — Екатеринбург: Б.и., 1996. – 64с.
5. Курош А. Г. Курс высшей алгебры: Учеб. для студентов вузов по спец. "Математика", "Приклад. математика". – 13-е изд., стер. – СПб.: Лань, 2004. – 432с.
6. Курош А. Г. Лекции по общей алгебре: учебник. – СПб.: Лань, 2005. – 560 с.
7. Гришина А.А. Подалгебры матричной алгебры $M_3(GF(2))$. Дипломная работа. УрГПУ. Екатеринбург. 2003.
8. Васильев С.А. Использование прикладного пакета GAP для описания решеток подалгебр моногенных трехмерных алгебр над полем $GF(2)$. Дипломная работа. УрГПУ. Екатеринбург. 2016.
9. Бочарова Т.С. Использование прикладного пакета GAP для описания решеток подалгебр трехмерных алгебр над полем $GF(2)$. Дипломная работа. УрГПУ. Екатеринбург. 2016.
10. Система компьютерной алгебры GAP – Exponenta. Режим доступа: www.exponenta.ru/soft/others/gap/1.asp
11. GAP Manual. Режим доступа: <http://www.gap-system.org/Doc/manuals.html>

Приложение

Массив матриц алгебры $A = M_3(GF(2))$

[illegible]

60

61

62

63

64

65

66

67

68